(b)

ELECTRONIC CHECK SYSTEM

Patent Number: JP9218905
Publication date: 1997-08-19

Inventor(s): YOSHIDA AKIO; IEGI TOSHIATSU; ICHIHARA NAOHISA
Applicant(s): N T T DATA TSUSHIN KK

Requested Patent: ☐ JP9218905
Application Number: JP19960022380 19960208
Priority Number(s):
IPC Classification: G06F19/00; G07F7/08
EC Classification:
Equivalents: JP3365599B2

Abstract

PROBLEM TO BE SOLVED: To detect the copy use of an electronic check by communication between interested parties and to make a payment by a received electronic check.
SOLUTION: The secret key and public key of each user and the public key of a bank are stored in an IC card possessed by the user. When the user 11 sends the electronic check to the other user 27, the respective public keys are mutually informed between the IC cards 45 and 47 and a random number is informed from the IC card 47 of a receiver 27 to the IC card 45 of a payer 11. The IC card 45 on a paying side changes the sequence of a progression included in the electronic check based on the random number, ciphers it by the public key of the receiver 27 and transmits it to the IC card 47 on a receiving side. The IC card 47 on the receiving side deciphers the electronic check by the secret key of the receiver 27, confirms the propriety of a bank signature by the public key of the bank, confirms whether or not the sequence of the progression is correctly changed corresponding to the random number and formally receives the electronic check.

(b)

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－218905

(43)公開日　平成９年(1997)８月19日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ　19/00			Ｇ０６Ｆ　15/30	３６０	
Ｇ０７Ｆ　7/08				３５０	
			Ｇ０７Ｆ　7/08	Ｒ	

審査請求　未請求　請求項の数11　ＯＬ　（全 21 頁）

(21)出願番号　特願平8－22380

(22)出願日　平成８年(1996)２月８日

(71)出願人　000102728
エヌ・ティ・ティ・データ通信株式会社
東京都江東区豊洲三丁目３番３号

(72)発明者　吉田　明雄
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　家木　俊温
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　市原　尚久
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

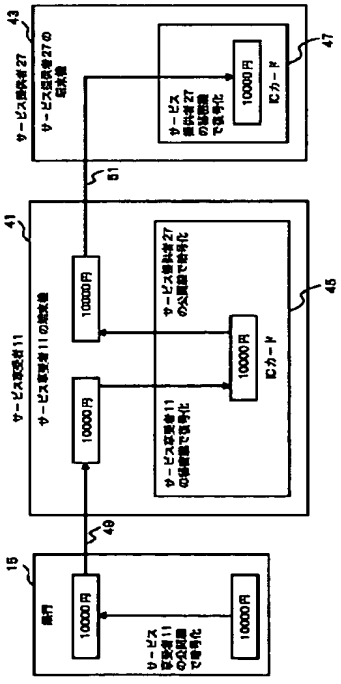
(74)代理人　弁理士　上村　輝之

(54)【発明の名称】　電子小切手システム

(57)【要約】　（修正有）

【課題】　当事者間の通信で電子小切手のコピー使用の検出ができ、受領した電子小切手で支払いが行える。

【解決手段】　利用者が所持するＩＣカードには、各々の利用者の秘密鍵、公開鍵及び銀行の公開鍵が記憶され、利用者１１が他の利用者２７へ電子小切手を送る場合は、ＩＣカード４５、４７間で各々の公開鍵が相互通知されると共に、受領者２７のＩＣカード４７から支払者１１のＩＣカード４５へ乱数が通知される。支払側ＩＣカード４５は、電子小切手に含まれている数列の順序を、乱数に基づいて変更した上で、受領者２７の公開鍵で暗号化して受領側ＩＣカード４７へ送信する。受領側ＩＣカード４７は、その電子小切手を受領者２７の秘密鍵で復号化し、銀行署名の正当性を銀行の公開鍵で確認し、数列の順序が乱数に従って正しく変更されているかを確認して、電子小切手を正式に受領する。



【特許請求の範囲】
【請求項１】　電子商取引に適用される電子小切手システムにおいて、
電子小切手の振出し及び決済を行う銀行のコンピュータと、前記電子小切手を利用する複数の利用者の各々が所持するＩＣカードとを備え、
前記銀行コンピュータが、振出した電子小切手に前記銀行の電子署名を含ませる署名手段を有し、
前記各利用者のＩＣカードが、
前記各利用者の秘密鍵を、ＩＣカード外部への読み出しが不可能な状態で記憶する秘密鍵記憶手段と、
前記各利用者の公開鍵及び前記銀行の公開鍵を記憶する公開鍵記憶手段と、
前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである支払者装置から電子小切手を受信するとき、前記支払者装置へ前記各利用者の公開鍵を送信する公開鍵送信手段と、
前記支払者装置から前記電子小切手を受信する小切手受信手段と、
前記受信した電子小切手を前記各利用者の秘密鍵を用いて復号化する小切手復号化手段と、
前記復号化した電子小切手に含まれている前記銀行の署名が正しいことを、前記銀行の公開鍵を用いて確認する署名確認手段と、
前記銀行署名が正しいことが確認されたとき、前記受信した電子小切手を受領したものとして記憶する小切手記憶手段と、
前記小切手記憶手段内の電子小切手を前記他の利用者のＩＣカードへ送信するとき、前記他の利用者のＩＣカードから前記他の利用者の公開鍵を受信する公開鍵受信手段と、
前記小切手記憶手段内の電子小切手を、前記受信した他の利用者の公開鍵によって暗号化する小切手暗号化手段と、
前記暗号化した電子小切手を、前記他の利用者のＩＣカードへ送信する小切手送信手段とを有することを特徴とする電子小切手システム。
【請求項２】　請求項１記載の電子小切手システムにおいて、
前記各利用者のＩＣカードが、前記利用者の秘密鍵と公開鍵とを生成する鍵生成手段をさらに有することを特徴とする電子小切手システム。
【請求項３】　請求項２記載の電子小切手システムにおいて、
前記銀行コンピュータが、前記ＩＣカードを利用者に発行する手段をさらに有し、
前記ＩＣカードの鍵生成手段が、発行されたときに前記利用者の秘密鍵と公開鍵とを生成して、生成した利用者の公開鍵を前記銀行のコンピュータに通知することを特徴とする電子小切手システム。
【請求項４】　請求項１、２及び３のいずれか一項に記載の電子小切手システムにおいて、
前記銀行コンピュータが、前記振出した電子小切手に、一定の順序で並んだ複数の数字を含ませる数字列付加手段をさらに有し、
前記各利用者のＩＣカードが、
前記他の利用者のＩＣカードから前記電子小切手を受信するとき、第１の乱数を発生させて前記他の利用者のＩＣカードに送信する乱数発生手段と、
前記受信した電子小切手に含まれている前記複数の数字の順序が、前記通知した第１の乱数に従って一定の規則の下で正しく変更されていることを確認する数字順序確認手段と、
前記小切手記憶手段内の電子小切手を、前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである受領者装置へ送信するとき、前記受領者装置が発生させた第２の乱数を前記受領者装置から受信する乱数受信手段と、
前記小切手記憶手段内の電子小切手に含まれている前記複数の数字を、前記受信した第２の乱数に従って前記一定の規則の下で変更する順序変更手段とを更に有し、
前記各利用者のＩＣカードの前記小切手記憶手段が、前記銀行署名が正しいことが確認されたのに加え、前記受信した電子小切手の数字順序が正しく変更されていることが確認されたとき、前記受信した電子小切手を受領したものとして記憶することを特徴とする電子小切手システム。
【請求項５】　請求項４記載の電子小切手システムにおいて、
前記銀行のコンピュータが、
前記銀行の秘密鍵を、銀行外部への読み出しが不可能な状態で記憶する銀行秘密鍵記憶手段と、
前記銀行の公開鍵及び利用者の公開鍵を記憶する銀行公開鍵記憶手段と、
前記振出した電子小切手を、前記利用者の公開鍵によって暗号化する振出小切手暗号化手段と、
暗号化した前記振出した電子小切手を、前記利用者のＩＣカードの一つへ送信する振出小切手送信手段と、
前記利用者のＩＣカードから決済対象の電子小切手を受信する決済小切手受信手段と、
前記受信した決済対象の電子小切手を前記銀行の秘密鍵を用いて復号化する決済小切手復号化手段と、
前記復号化した決済対象の電子小切手に含まれている前記銀行署名が正しいことを、前記銀行の公開鍵を用いて確認する銀行署名確認手段と、
前記決済対象の電子小切手の銀行署名が正しいことが確認されたとき、前記決済対象の電子小切手による決済を実行する決済実行手段と、
をさらに有することを特徴とする電子小切手システム。
【請求項６】　請求項５記載の電子小切手システムにお

いて、
前記銀行コンピュータが、
前記各利用者のＩＣカードから前記決済対象の電子小切手を受信するときに、
前記第２の乱数を発生させて前記ＩＣカードに通知する銀行乱数発生手段と、
前記受信した決済対象の電子小切手に含まれている前記複数の数字の順序が、前記通知した第２の乱数に従って一定の規則の下で正しく変更されていることを確認する銀行数字順序確認手段と、を更に有し、
前記銀行コンピュータの前記決済実行手段が、前記銀行署名が正しいことが確認されたのに加え、前記決済対象の電子小切手の数字順序が正しく変更されていることが確認されたとき、前記決済対象の電子小切手の決済を実行することを特徴とする電子小切手システム。
【請求項７】　電子商取引に適用される電子小切手システムにおいて、
電子小切手の振出し及び決済を行う銀行のコンピュータと、前記電子小切手を利用する複数の利用者の各々が所持するＩＣカードとを備え、
前記銀行コンピュータが、振出した電子小切手に、一定の順序で並んだ複数の数字を含ませる数字列付加手段を有し、
前記各利用者のＩＣカードが、
前記他の利用者のＩＣカードから電子小切手を受信する前に、第１の乱数を発生させて前記他の利用者のＩＣカードに送信する乱数発生手段と、
前記他の利用者のＩＣカードから前記電子小切手を受信する小切手受信手段と、
前記受信した電子小切手に含まれている前記複数の数字の順序が、前記通知した第１の乱数に従って一定の規則の下で正しく変更されていることを確認する数字順序確認手段と、
前記受信した電子小切手の数字順序が正しく変更されていることが確認されたとき、前記受信した電子小切手を受領したものとして記憶する小切手記憶手段と、
前記小切手記憶手段内の電子小切手を、前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである受領者装置へ送信する前に、前記受領者装置が発生させた第２の乱数を前記受領者装置から受信する乱数受信手段と、
前記小切手記憶手段内の電子小切手に含まれている前記複数の数字を、前記受信した第２の乱数に従って前記一定の規則の下で変更する順序変更手段と、
前記順序変更手段によって前記数字順序が変更された前記電子小切手を、前記受領者装置に送信する小切手送信手段と、を有することを特徴とする電子小切手システム。
【請求項８】　請求項７記載の電子小切手システムにおいて、
前記銀行コンピュータが、
前記各利用者のＩＣカードから決済対象の電子小切手を受信する前に、前記第２の乱数を発生させて前記ＩＣカードに通知する銀行乱数発生手段と、
前記各利用者のＩＣカードから前記決済対象の電子小切手を受信する決済小切手受信手段と、
前記受信した決済対象の電子小切手に含まれている前記複数の数字の順序が、前記通知した第２の乱数に従って一定の規則の下で正しく変更されていることを確認する銀行数字順序確認手段と、
前記決済対象の電子小切手の数字順序が正しく変更されていることが確認されたとき、前記決済対象の電子小切手の決済を実行する決済実行手段とを有することを特徴とする電子小切手システム。
【請求項９】　請求項７に記載の電子小切手システムにおいて、
前記複数の数字の各々が乱数であることを特徴とする電子小切手システム。
【請求項１０】　銀行のコンピュータから振出された電子小切手であって、前記銀行の電子署名が付与されている電子小切手を格納するために、複数の利用者の各々が所持するＩＣカードにおいて、
前記各利用者の秘密鍵を、ＩＣカード外部への読み出しが不可能な状態で記憶する秘密鍵記憶手段と、
前記各利用者の公開鍵及び前記銀行の公開鍵を記憶する公開鍵記憶手段と、
前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである支払者装置から電子小切手を受信するとき、前記支払者装置へ前記各利用者の公開鍵を送信する公開鍵送信手段と、
前記支払者装置から前記電子小切手を受信する小切手受信手段と、
前記受信した電子小切手を前記各利用者の秘密鍵を用いて復号化する小切手復号化手段と、
前記復号化した電子小切手に含まれている前記銀行の署名が正しいことを、前記銀行の公開鍵を用いて確認する署名確認手段と、
前記銀行署名が正しいことが確認されたとき、前記受信した電子小切手を受領したものとして記憶する小切手記憶手段と、
前記小切手記憶手段内の電子小切手を前記他の利用者のＩＣカードへ送信するとき、前記他の利用者のＩＣカードから前記他の利用者の公開鍵を受信する公開鍵受信手段と、
前記小切手記憶手段内の電子小切手を、前記受信した他の利用者の公開鍵によって暗号化する小切手暗号化手段と、
前記暗号化した電子小切手を、前記他の利用者のＩＣカードへ送信する小切手送信手段とを有することを特徴とする電子小切手システム用のＩＣカード。

【請求項１１】　請求項１０記載のＩＣカードにおいて、
電子小切手には、一定の順序で並んだ複数の数字が含まれており、
前記各利用者のＩＣカードが、
前記他の利用者のＩＣカードから前記電子小切手を受信するとき、第１の乱数を発生させて前記他の利用者のＩＣカードに送信する乱数発生手段と、
前記受信した電子小切手に含まれている前記複数の数字の順序が、前記通知した第１の乱数に従って一定の規則の下で正しく変更されていることを確認する数字順序確認手段と、
前記小切手記憶手段内の電子小切手を、前記銀行コンピュータ及び他の利用者のＩＣカードのいずれかである受領者装置へ送信するとき、前記受領者装置が発生させた第２の乱数を前記受領者装置から受信する乱数受信手段と、
前記小切手記憶手段内の電子小切手に含まれている前記複数の数字を、前記受信した第２の乱数に従って前記一定の規則の下で変更する順序変更手段とを更に有し、
前記各利用者のＩＣカードの前記小切手記憶手段が、前記銀行署名が正しいことが確認されたのに加え、前記受信した電子小切手の数字順序が正しく変更されていることが確認されたとき、前記受信した電子小切手を受領したものとして記憶することを特徴とする電子小切手システム用のＩＣカード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、通信ネットワークを通じた商取引（電子商取引という）に適用される電子小切手システムの改良に関するものである。
【０００２】
【従来の技術】従来、商取引においては、現金や手形、小切手のように特定の紙類や金属類等に貨幣価値を化体させた物理的媒体をベースとして、決済が行われてきた。
【０００３】しかし、近年、通信ネットワークの急速な発達によって、あらゆる情報の授受が通信ネットワークを通じて行われるようになり電子商取引と称される、通信ネットワークを通じた商取引が実現可能になると、電子商取引の当事者間において上記物理的媒体の占有を移転する方法以外の決済方法が必要になってくる。
【０００４】そこで、図１に示すような電子小切手システムが、特開平６－１６２０５９号公報において開示され、この電子小切手システムに関して検討が行われている。
【０００５】
【発明が解決しようとする課題】ところで、上記電子小切手システムにおいては、電子小切手は単なる「０」と「１」とのビット列で表される情報となってしまう。そのため、それら情報のコピーや偽造をどのような方法で防止するのか、及び、取引の相手方の確認や電子小切手の授受等が暗号技術によって行われる際に、使用される鍵の管理の安全性をどのような方法で確保するのかが最も重要な問題になってくる。
【０００６】例えば、上記システムを示した図１において、支払者３が通信ネットワークを通じて銀行１に、１万円の電子小切手の発行依頼を送信したとする。銀行１ではこの発行依頼を受信すると、支払者３の口座から１万円を引き落とすと共に、支払者３に、電子小切手で１万円を支払うこととなる。
【０００７】この電子小切手による支払に際して、銀行１から通信ネットワークを通じて送信されてくる１万円の情報が、仮に支払者３にも解読できない態様で暗号化されていたとしても、支払者３がこの情報を受信したままの態様でコピーすることは極めて簡単に行える。しかも、支払者３にはこの情報の中身が判らなかったとしても、この情報が１万円の価値があることが判っている。
【０００８】そのため、支払者３は、この１万円の電子小切手をコピーしておき、商店５に対する支払いだけでなく商店７に対する支払いに使用しても、商店７ではその電子小切手がコピーされたものか否かの判定は行えない。また、商店５もこの電子小切手をコピーして、他者（図示しない）への支払いに重複使用することが可能である。
【０００９】そこで、上記システムでは同一電子小切手の２重使用を防止するための方法として以下のような対策を講じている。即ち、発行済み電子小切手を一元的に登録する証明機関を設け、この証明機関に通信ネットワークを通じて電子小切手を格納した金銭モジュールを定期的にアクセスさせて電子小切手の重複使用や不正使用のチェックを受けるよう、電子小切手所有者に義務付けている。
【００１０】しかし、この方法では、不特定多数の個人が電子小切手を所有するようになると、証明機関の負荷が非常に大きくなる。また、電子小切手の使用が証明機関の運転時間によって制約を受けたり、仮に証明機関が２４時間運転を行っている場合でも証明機関がダウンしたときは、電子小切手が使用できないという問題点が生ずる。更に、不特定多数の個人が比較的低い金額の電子小切手の授受を多数回行うような場合には、証明機関に対する通信コストの負担割合が増大するという問題点も生ずる。
【００１１】従って本発明の第１の目的は、電子小切手所有者が多数存在するシステムにおいて、取引の当事者間だけの通信（つまり、オフライン通信）で電子小切手のコピー使用の検出ができ、受領した電子小切手で他者にも支払いが行える電子小切手システムを提供することにある。
【００１２】また、本発明の第２の目的は、取引の相手

方の確認や電子小切手の授受等が暗号技術によって行われる際に、使用される鍵の管理が安全、容易で且つ、振出人の署名の確認が行える電子小切手システムを提供することにある。

【００１３】

【課題を解決するための手段】本発明の第１の側面に従う電子小切手システムは、電子小切手の振出し及び決済を行う銀行のコンピュータと、その電子小切手を利用する複数の利用者の各々が所持するＩＣカードとを備える。銀行コンピュータは、電子小切手を振出すとき、その電子小切手にその銀行の電子署名を付与する。各利用者のＩＣカードは、それぞれの利用者の秘密鍵及び公開鍵と、銀行の公開鍵とを記憶している。各利用者の秘密鍵は、それぞれのＩＣカード外へ漏れることはないよう、ＩＣカード内で秘密に保持されている。

【００１４】各利用者が銀行又は他の利用者から電子小切手を受領するときは、当該利用者のＩＣカードが、その小切手支払者の装置つまり銀行コンピュータ又は他の利用者のＩＣカードと通信可能に接続され、そして、その支払者装置に対し当該利用者の公開鍵を送信し、且つ、その支払者装置から前記電子小切手を受信する。次に、当該利用者のＩＣカードは、受信した電子小切手を当該各利用者の秘密鍵を用いて復号化し、続いて、その復号化した電子小切手に含まれている銀行署名が正しいことを、その銀行の公開鍵を用いて確認する。その結果、銀行署名が正しいことが確認されると、その受信した電子小切手を正式に受領して記憶する。

【００１５】一方、各利用者が電子小切手を他の利用者へ渡そうとする時は、当該利用者のＩＣカードは相手のＩＣカードと通信可能に接続され、そして、まず、その相手ＩＣカードからその相手の公開鍵を受信し、次に、その受信した相手の公開鍵を用いて送信対象の電子小切手を暗号化し、そしてこの暗号化した電子小切手を相手カードへ送信する。相手カードは、上記した小切手受領時の動作と同じ処理を行うことにより、その送信された電子小切手の署名の正当性を確認し、そして正式に受領する。

【００１６】このように、本システムでは、電子小切手を授受するときの鍵の通信は、小切手授受を行う当事者が、第３者と通信することなしに、各々の公開鍵を相手に通知するだけで済むため、鍵の管理が容易である。

【００１７】また、本発明の第２の側面に従う電子小切手システムは、電子小切手の振出し及び決済を行う銀行のコンピュータと、その電子小切手を利用する複数の利用者の各々が所持するＩＣカードとを備える。銀行コンピュータは、電子小切手を振出すとき、その電子小切手に一定の順序で並んだ複数の数字を付与する。また、各利用者のＩＣカードは、他の利用者のＩＣカードから電子小切手を受信するとき、まず乱数を発生させて相手のＩＣカードに送信する。相手のＩＣカードは、その乱数に応じて、送信対象の電子小切手内の複数数字の順序を一定の規則の下で変更し、その後に、その電子小切手を当該利用者のＩＣカードへ送信する。当該利用者のＩＣカードは、相手から受信した電子小切手内の複数数字の順序が、自分が相手に送った乱数に従って正しく変更されているか否かをチェックし、正しいことが確認された場合にのみ、その電子小切手を正式に受領する。

【００１８】このようにすると、もし、ある利用者が過去の支払で送信済みの電子小切手をコピーしておき、このコピーを別の支払の為に再度送信した場合、そのコピーに含まれている複数数字の順序は過去の送信時の乱数に基づいて変更されたものであるから、今回の送信時の乱数に基づく順序とは異なることになる。よって、そのコピーの受領は拒否され、電子小切手の不法な二重使用が防止される。

【００１９】好適な実施形態では、上記２つのシステムの双方の構成が組み合わされる。この実施形態では、銀行コンピュータが利用者のＩＣカードから電子小切手を受け取るときも、上述した利用者ＩＣカード同士の電子小切手授受のときと同様の態様で、受け取った電子小切手の署名確認と数字列順序の確認とを行なう。

【００２０】

【実施の形態】まず、本発明の電子小切手システムの原理的背景について説明する。

【００２１】この種の電子小切手システムでは暗号処理は必須であり、特に、本発明に係るシステムでは、通信文を暗号化するだけでなく通信文に署名（電子署名）を施し、相手（即ち、送信元）を確認する機能を有する公開鍵暗号方式が用いられている。

【００２２】この公開鍵暗号を利用して相手を確認する方式は、特開昭６０－２６３７８号（ディジタル署名方式）等に開示されている通りである。即ち、原理的には送信者側が通信文を圧縮し、この圧縮したデータに対し秘密鍵によって復号化処理を行い、これを認証子として通信文と共に相手方（受信者側）に送る。その通信文及び認証子を受け取った相手方は、その認証子を相手の公開鍵で暗号化した結果と、通信文を送信者側で圧縮したのと同じ方法で圧縮した結果とが同一であるかどうかをチェックする。これによって上記通信文が正しい相手から（秘密鍵を有している相手から）送信されたものであることを確認することができる。

【００２３】次に、上述した原理を、本発明の一実施形態に係る電子小切手システムを示す図２を参照して具体的に説明する。この図２では、簡単のため、電子小切手システムの構成要素を単純化して示している。

【００２４】上記システムは、図示のように、サービス享受者（例えば買物客）１１、銀行１５、サービス享受者１１の銀行口座１７、銀行１５の払出小切手支払口座２１、サービス提供者（例えば商店）２７、及びその銀行口座３５から構成される。サービス享受者１１及びサ

ービス提供者２７は、それぞれＩＣカード（図示しない）を所有し、それらＩＣカードが電子小切手や秘密鍵及び公開鍵等を所持するための媒体として用いられる。

【００２５】図２において、まず、サービス享受者１１が、矢印１３で示すように銀行１５に対し電子小切手の振出しを依頼すると、銀行１５は、サービス享受者１１から要求された金額以上の残高が口座１７にあるか否かを確認する。この結果、上記残高が口座１７にあれば、要求金額を矢印１９で示すように口座１７から銀行１５の払出小切手支払口座２１に移すと共にサービス享受者１１に対し、矢印２３で示すように銀行振出の電子小切手を発行する。

【００２６】サービス享受者１１は、この振出された電子小切手の正当性が確認できたならば、この電子小切手を受領する（ここで、銀行振出の小切手とする理由は、暗号鍵の管理を容易にすると共に、この小切手により支払いを受ける者に対して支払保証を確実にするという目的があるためである）。

【００２７】次に、サービス享受者１１は、矢印２５で示すようにサービス提供者２７からサービスの提供を受けたり商品の購入等を行って、それらの購入代金を矢印２９で示すようにサービス提供者２７に対し電子小切手で支払う。サービス提供者２７は、この電子小切手が銀行振出の正当な小切手であることが確認できたならば、この電子小切手を受領する。その後、サービス提供者２７は、矢印３１で示すように銀行１５に対し、サービス享受者１１から受領した電子小切手を呈示し、支払を要求する。

【００２８】銀行１５は、サービス提供者２７が呈示した電子小切手の正当性を確認し、その結果、自己振出の電子小切手であることが確認できたならば、矢印３３で示すように額面金額を払出小切手支払口座２１からサービス提供者２７の口座５に振替える。

【００２９】上述した電子小切手システムを実現するには、銀行１５、サービス享受者１１、サービス提供者２７が夫々秘密鍵と公開鍵とを所有し、取引の都度相手の署名を確認する必要がある。また、自己の秘密鍵を隠蔽することが重要であると共に、通信相手の公開鍵の入手も容易でなければならない。

【００３０】上記システムにおいて、銀行１５は通常、自身の業務を効率的に行うために、コンピュータセンタ（図示しない）を備えている。従って、銀行１５の秘密鍵や公開鍵は、そのコンピュータセンタの中に置くこともできる（勿論、この秘密鍵は厳重なる注意を持って管理されなければならない）。しかし、サービス享受者１１やサービス提供者２７は、その多くが個人であることから、銀行１５のようなコンピュータセンタを所有することはできず、その秘密鍵の管理方法が問題となる。

【００３１】そこで、サービス享受者１１やサービス提供者２７には、耐タンパー性（つまり、内部データの不法改変が事実上不可能であること）を有するＩＣカードに秘密鍵を格納して所有させることとする。ここで、耐タンパー性を有するＩＣカードとは、少なくともＣＰＵ、メモリ、入出力ポート等から構成されるもので、そのメモリには外部から直接アクセスすることができず、メモリに対するアクセスはＣＰＵが制御し、入出力ポートを経由して外部とデータ交換を行う構成のＩＣカードである。

【００３２】上述した理由から、サービス享受者１１やサービス提供者２７は、自身の秘密鍵を格納したＩＣカードを所有する必要があるが、これは以下の方法で入手することができる。

【００３３】まず、サービス享受者１１やサービス提供者２７は、事前に銀行１５に夫々口座１７、３５を開設しておき、銀行１５に電子小切手システムを利用する旨の要求を行う。銀行１５は、サービス享受者１１やサービス提供者２７の本人確認や資格確認等を行った後、これら利用者（１１、２７）の秘密鍵を格納したＩＣカードを発行する。

【００３４】これらＩＣカードには、秘密鍵の他、銀行１５が発行した正当なＩＣカードだけが有する署名情報や利用者（１１、２７）のＩＤや公開鍵、銀行１５の公開鍵や銀行１５が振出した電子小切手の署名を確認する関数や通信文を暗号化、復号化する関数、受領した電子小切手を格納し管理するための機能等が必要となる。これらの機能は、ＩＣカード内にプログラムとして組込むことで実現できる。

【００３５】なお、利用者（１１、２７）の鍵生成については、銀行１５内で利用者（１１、２７）の秘密鍵、公開鍵を生成することもできるが、銀行１５自身が関与しない形で秘密鍵や公開鍵を生成でき、特に利用者（１１、２７）の秘密鍵については銀行１５にも利用者（１１、２７）本人にも知り得ない形態を取るのが望ましい。この方法としては、ＩＣカード内でＣＰＵが独自に利用者（１１、２７）の秘密鍵と公開鍵とを生成して公開鍵だけ銀行１５に通知する方法がある。また、ＩＣカードの処理能力では鍵生成が困難な場合、銀行１５で利用者（１１、２７）の公開鍵と秘密鍵とを生成させるが、利用者（１１、２７）の秘密鍵は、ＩＣカードだけに記憶させ、銀行１５では保持しないようにしておくことが望ましい。いずれにしても、銀行１５のコンピュータセンタが、発行したＩＣカードの利用者ＩＤ、及び公開鍵を記憶しておくこととなる。また、利用者（１１、２７）の秘密鍵は、個々の利用者のＩＣカードのＩＣチップ内に、ＩＣチップ外へ読出すことが不可能な状態で格納される。

【００３６】このようにして発行されたＩＣカードを使用して、銀行１５とサービス享受者１１やサービス提供者２７、或いは、サービス享受者１１とサービス提供者２７との間で電子小切手の授受が行われることとなる。

【００３７】まず、図２において、サービス享受者１１が銀行１５から電子小切手を振出す場合、銀行１５は、電子小切手を構成するデータを生成し、これに銀行１５の電子署名を付与する。そして、この電子署名を付した電子小切手全体を、サービス享受者１１の公開鍵で暗号化した後、サービス享受者１１のＩＣカードに送る。サービス享受者１１のＩＣカードは、暗号化された電子小切手全体を受け取ると、自身の秘密鍵を使用して復号化し、銀行１５の公開鍵を使用して銀行１５の証明を確認する。

【００３８】このとき、銀行１５では、サービス享受者１１の利用者ＩＤに基づいてサービス享受者１１の公開鍵を検索する必要があるが、公開鍵であるため厳重なセキュリティは要求されない。また、サービス享受者１１のＩＣカードは、自身のチップ内に格納された秘密鍵を外部に漏らすことなく上記データを復号化し、自身に記憶されている銀行１５の公開鍵を使用して銀行１５の電子署名を確認することができる。

【００３９】次に、図２において、サービス享受者１１が銀行１５振出の電子小切手をサービス提供者２７に支払う場合について説明する。

【００４０】サービス享受者１１のＩＣカード及びサービス提供者２７のＩＣカードは、夫々銀行１５から発行されたときに埋め込まれた正当性を示す銀行１５の署名情報や秘密情報を有することを確認することによって相互認証を行う。相互に正当な通信相手であることを確認した２枚のＩＣカードは、互いの公開鍵を交換し合う。サービス享受者１１のＩＣカードは、銀行１５の電子署名の付いた電子小切手をサービス提供者２７の公開鍵で暗号化し、サービス提供者２７のＩＣカードに送る。サービス提供者２７のＩＣカードは、自身の秘密鍵を外部に漏らすことなく上記データを復号化し、自身に記憶されている銀行１５の公開鍵を使用して銀行１５の電子署名を確認する。サービス提供者２７は、銀行１５の電子署名が確認できることでその電子小切手が銀行１５から発行されたものであることが確認できる。更に、サービス提供者２７は、同様の方法で正当に発行されたＩＣカードを持つ第三者に対し、サービス享受者１１から受領した電子小切手で支払いを行うことが可能である。

【００４１】ここで、電子小切手の振出人を銀行１５としておけば、夫々のＩＣカードに共通的に存在する銀行１５の公開鍵を使用して銀行１５の電子署名を確認することができ、鍵の管理が非常に楽になる。なお、電子小切手の振出人を銀行１５への要求者であるサービス享受者１１とすることもできるが、サービス享受者１１の電子署名を確認するためのサービス享受者１１の公開鍵を入手する手段が問題となる。

【００４２】即ち、サービス享受者１１からサービス提供者２７にサービス享受者１１の公開鍵を渡す場合、サービス享受者１１が不正を働き、独自に生成した秘密鍵と公開鍵とを用いて電子署名を行い、その公開鍵をサービス提供者２７に送ったとしても、サービス提供者２７はサービス享受者１１が不正を働いたかどうか判定することができない。従って、サービス提供者２７のＩＣカードは、サービス享受者１１と取引する以前にサービス享受者１１の公開鍵を所持しているか、銀行１５又は公正な第三者機関（図示しない）からサービス享受者１１のＩＣカードの公開鍵を入手する必要がある。これは、不特定多数人が取引するシステムでは実現困難である。

【００４３】また、社会通念上、不特定多数の個人であるサービス享受者１１が振出した小切手よりも、銀行１５が振出した小切手の方が信用度が高い。仮に、サービス享受者１１とサービス提供者２７との間で従来から取引関係があり、サービス享受者１１が振出した小切手をサービス提供者２７が受け入れたとしても、サービス享受者１１振出しの小切手をサービス提供者２７が第三者（図示しない）に支払う場合、サービス享受者１１と第三者との間で信用関係がなければ、第三者はサービス享受者１１振出の小切手を受領することを拒むかもしれない。

【００４４】このようにして発行された２枚のＩＣカードを使用して、サービス享受者１１やサービス提供者２７は、銀行１５との間で電子小切手の受領や決済を行うが、これら２枚のＩＣカードと銀行１５との間で直接やり取りができる訳ではない。

【００４５】これら２枚のＩＣカードと銀行１５との間で、電子小切手の受領や決済を行う手段としては、以下のような方法が考えられる。

【００４６】（１）銀行１５の窓口に上記ＩＣカードを呈示する方法。

【００４７】（２）上記のような電子小切手システムに対応したＡＴＭを使用する方法。

【００４８】（３）２枚のＩＣカードと通信を行う機能、２枚のＩＣカードとの間で授受される情報の表示機能、操作者の意思等を２枚のＩＣカードに伝達するための入力機能、及び銀行１５と通信を行う機能を少なくとも備える端末機を使用する方法。

【００４９】特に（３）の方法では、これに適用される端末機を、市販のパーソナルコンピュータ（パソコン）、ＩＣカードリーダ／ライタ（ＩＣカードＲ／Ｗ）、モデム等を組合せて実現することができるので、サービス享受者１１はこの端末機を用いて自宅や勤務先等から電子小切手の受領や決済を行うこともできる。

【００５０】更に、（３）の条件を満足するために、持ち運び可能な携帯用端末機と移動体通信とを組合せることで、外出先等からでも電子小切手の受領や決済を行うこともできるようになる。

【００５１】また、サービス享受者１１とサービス提供者２７との間における電子小切手の支払いや受領には、以下のような方法が考えられる。

【００５２】（４）サービス提供者２７の店舗内に、少なくともサービス享受者１１のＩＣカードとサービス提供者２７のＩＣカード間での通信機能、情報の表示機能、操作者の意思等を伝えるための入力機能を備えた端末機を使用する方法。
【００５３】（５）上記（３）に示した端末機を使用する方法。
【００５４】（６）上記（４）及び（５）を組合せた端末機を使用する方法。
【００５５】（４）の方法は、サービス享受者１１がサービス提供者２７の店舗に出向き、ここで電子小切手の支払いを行う場合に使用される。
【００５６】（５）の方法では、サービス享受者１１又はサービス提供者２７の一方が遠隔地におり、通信ネットワークを介した状態で電子小切手の支払いが行える。例えば、インターネットを介して情報提供者から有料の情報を受け取り、電子小切手によりその代金の支払いを行う場合等が思料される。
【００５７】このように、利用者（サービス享受者１１、サービス提供者２７）毎の暗号処理に必要な機能をＩＣカード内に組込むことで、上記電子小切手システムに使用する端末機に対し、鍵の管理等に対する要求条件がなくなるため、端末機の設計の自由度が増え、時代の要請にあった電子小切手システムの構築がし易くなる。
【００５８】ところで、上記システムにおいては、銀行１５から受領した電子小切手がサービス享受者１１からサービス提供者２７に支払われるとき、サービス提供者２７がサービス享受者１１以外と通信せずに（つまりオフラインで）、支払われた電子小切手の不正使用をどのように検出するかが、本質的な課題である。
【００５９】次に、上記システムにおける発行済み電子小切手の重複使用の防止方法を、図３を参照して説明する。
【００６０】図３は、上記電子小切手システムを構成するサービス享受者１１、銀行１５、及びサービス提供者２７を示す拡大図である。図から明らかなように、サービス享受者１１は上述した（３）の方法に適用される専用の端末機４１及び専用のＩＣカード４５を所有し、サービス提供者２７も同様の構成の端末機４３及び専用のＩＣカード４７を所有している。そして、端末機４１、４３間や端末機４１、４３と銀行１５の端末機との間は、通信ネットワークによって接続可能に構成されているものとする。
【００６１】図３において、符号４９では、銀行１５から振出された例えば１万円の電子小切手はサービス享受者１１の公開鍵で暗号化される。この暗号化されたデータは、ＩＣカード４５内でサービス享受者１１の秘密鍵によって復号化され、サービス提供者２７に支払われるとき（符号５１で示す）は、サービス提供者２７の公開鍵で暗号化される。
【００６２】この場合、符号４９の時点でのデータを、サービス享受者１１本人又は第三者がコピーしておいて、そのままの形でサービス提供者２７に支払ってもＩＣカード４７は正しいデータに戻すことができないから、この電子小切手の受領は拒否される。なお、サービス享受者１１の秘密鍵はＩＣカード４５内にあり、ＩＣカード外へは読出し不可能なので、サービス享受者１１自身もこの暗号文４９を復号化することはできない。
【００６３】しかし、符号５１の時点でのデータを、サービス享受者１１本人又は第三者がコピーしておき、再度サービス提供者２７に支払った場合、ＩＣカード４７は正しいデータに復号してしまう。ＩＣカード４７で、このデータがオリジナルか不法コピーかを判断するためには、過去に受領した電子小切手を記憶しておき、これを検索することが必要となるが、ＩＣカードには無限のメモリを搭載できる訳ではないので、現実的ではない。
【００６４】そこで、図４に示すように、銀行１５は、１万円の電子小切手を振出す際に、１万円の電子小切手データに値の異なるｎ個の乱数ｒｂｎｋ１、ｒｂｎｋ２、…、ｒｂｎｋｎを付与し、サービス享受者１１の公開鍵で暗号化し、ＩＣカード４５に送信する。
【００６５】この暗号化されたデータを受信すると、ＩＣカード４５は自身の秘密鍵で復号化して１万円の電子小切手とする。そして、ＩＣカード４５はこの電子小切手をＩＣカード４７に移すときに、まず、ＩＣカード４７から値の異なるｎ個の乱数ｒｂ１、ｒｂ２、…、ｒｂｎを貰う。次に、これら乱数ｒｂ１、ｒｂ２、…、ｒｂｎの受信順序（並び順序）と大きさとによって銀行１５で付与されたｒｂｎｋ１、ｒｂｎｋ２、…、ｒｂｎｋｎの並びを一定の規則で変更する。その後、サービス提供者２７の公開鍵で暗号化し、ＩＣカード４７へ送信する。
【００６６】ＩＣカード４７では、ＩＣカード４５から受信した電子小切手データを復号化した後、自分が送信した乱数の順序と大きさの関係とｒｂｎｋ１、ｒｂｎｋ２、…、ｒｂｎの並び順の関係が規則に従って変更されているか否かを検査し、規則に従っていないときは、この電子小切手の受領を拒否する。従って、サービス享受者１１がＩＣカード４５から出力された符号５１の時点でのデータをコピーしておいても、ＩＣカード４７から発生する乱数ｒｂ１、ｒｂ２、…、ｒｂｎの順序と大きさとの関係がコピーした時点と一致しない限り使用することができない。
【００６７】ここで、符号５１の時点でのデータをコピーしたサービス享受者１１がサービス提供者２７と正常に取引できる確率は、１／ｎ！である。具体例を示せば下記の通りであるから、乱数の数ｎは、７個程度以上あれば実用上問題ないであろう。
【００６８】

確率（ｎ＝5）＝1／5！＝1／120　≒0．83%
確率（ｎ＝6）＝1／6！＝1／720　≒0．14%
確率（ｎ＝7）＝1／7！＝1／5040　≒0．02%
確率（ｎ＝8）＝1／8！＝1／40320　≒0．002%
確率（ｎ＝9）＝1／9！＝1／362880≒0．0003%

なお、図示のシステムでは、ｒｂｎｋ1～ｒｂｎｋｎは、5個の乱数とし、ｒｂｎｋ1～ｒｂｎｋ5の大小関係はｒｂｎｋ1＜ｒｂｎｋ2＜ｒｂｎｋ3＜ｒｂｎｋ4＜ｒｂｎｋ5としてある。ＩＣカード45は、ＩＣカード47からｒｂ1、ｒｂ2、ｒｂ3、ｒｂ4、ｒｂ5の順で乱数を受信する。そして、ｒｂ1＝1、ｒｂ2＝4、ｒｂ3＝2、ｒｂ4＝5、ｒｂ5＝3であるとすると、ＩＣカード45は、上記乱数をｒｂｎｋ1、ｒｂｎｋ4、ｒｂｎｋ2、ｒｂｎｋ5、ｒｂｎｋ3の順に並び変えてＩＣカード47に送信する。

【0069】次に、上記システムを利用するのに必要な電子小切手台帳（つまり、ＩＣカード）の発行手順を、図5のフローチャートを参照して説明する。

【0070】電子小切手の利用者であるサービス享受者11及びサービス提供者27は、銀行15から電子小切手台帳としてのＩＣカードを発行して貰う必要がある。銀行15がサービス享受者11にＩＣカードを発行する際の手順を以下に示す。この手順はサービス提供者27にＩＣカードを発行する際にも適用される。

【0071】まず、ＩＣカード発行の準備として、電子小切手の発行銀行となる銀行15は、電子小切手の署名に必要な公開鍵ＫＰＢＮＫと秘密鍵ＫＳＢＮＫとを生成しておき、公開鍵ＫＰＢＮＫを公開しておく。また、秘密鍵ＫＳＢＮＫについては、厳重な管理の下に置かれるようにしておく。

【0072】ステップＳ101において、サービス享受者11は銀行15に対し、ＩＣカードの発行を要求し、この要求を受けると銀行15は、ステップＳ102においてサービス享受者11の本人確認を行い、要求者がサービス享受者11本人であれば、サービス享受者11の口座の有無を調べる。サービス享受者11が口座を持っていなければ口座を開設させる。なお、銀行15がサービス享受者11に対して本人確認を行う方法は、免許証等の公的証明書、銀行15発行の通帳と印鑑、暗証番号等の本人しか知らない秘密情報を知っていることによる確認、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せて行う。

【0073】次に、ステップＳ103において、銀行15はサービス享受者11のために発行するＩＣカード45に対し、自身の公開鍵ＫＰＢＮＫ、秘密鍵ＫＳＢＮＫ、利用者ＩＤ（ＩＤａ）を通知する。そして、ＩＣカード45に対し、サービス享受者11個人の公開鍵ＫＰＡと秘密鍵ＫＳＡの発行、及び利用者ＩＤ（ＩＤａ）と公開鍵ＫＰＡに対する署名Ｓａの生成を依頼する。なお、ＩＣカード45は、署名Ｓａを生成後、銀行15の秘密鍵ＫＳＢＮＫは破棄する。ＩＣカード45に鍵生成能力が無い場合には、公開鍵ＫＰＡ及び秘密鍵ＫＳＡの生成や公開鍵ＫＰＡに対する署名Ｓａの生成は銀行15のセンタで行う。

【0074】次に、ステップＳ104において、鍵の生成依頼を受けたＩＣカード45は、サービス享受者11個人の公開鍵ＫＰＡと秘密鍵ＫＳＡとを生成した後、利用者ＩＤ（ＩＤａ）と公開鍵ＫＰＡに対する署名Ｓａとを、銀行15の秘密鍵ＫＳＢＮＫにより生成する。ＩＣカード45は、ＫＰＢＮＫ、ＫＳＡ、ＫＰＡ、ＩＤａ、Ｓａを記憶すると共に、銀行15に対して公開鍵ＫＰＡを通知する。なお、ＩＣカード45で個人の公開鍵、秘密鍵を生成する場合は、鍵生成依頼時の日付時刻、乱数等を使用して同じ鍵が生成されないようにする必要がある。

【0075】次に、ステップＳ105において、銀行15は、ＩＤａと公開鍵ＫＰＡを記憶しておく。

【0076】次に、上記のようにして発行されたＩＣカードを用いて行われる電子小切手の振出しを、図6、及び図7のフローチャートを参照して説明する。

【0077】図6、及び図7は、サービス享受者11が銀行15に対して、電子小切手の振出しを依頼する場合の手続を示す。

【0078】まず、ステップＳ111において、サービス享受者11は、ＩＣカード45が使用できる銀行15のＡＴＭ又は銀行15と通信ネットワークを通じて通信が可能で且つ電子小切手台帳であるＩＣカード45が使用できる端末機41を経由して、銀行15に対し電子小切手の振出依頼を行う。なお、ＩＣカード45とサービス享受者11及び銀行15とは実際にはＡＴＭ又は端末機41を介して通信を行うがこれらの装置は情報を中継するだけであるため、以降の説明からは省略する。

【0079】次に、ステップＳ112において、振出要求を受けたＩＣカード45は、サービス享受者11に対してサービス享受者11の本人確認を行う。本人確認の方法は、暗証番号、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せて行う。その後、ステップＳ113において、ＩＣカード45は本人確認が行えたならば、銀行15に対し、ＩＤａからの電子小切手振出し要求を通知する。

【0080】次に、ステップＳ114において、ＩＣカード45と銀行15は、相互に認証を行い、互いに正当な通信相手であることを確認する。例えば、ここでは、次のような方式で相互の認証を行うことが可能である。ＩＣカード45は、ＫＳＡ、ＩＤａ、Ｓａを銀行15の

公開鍵ＫＰＢＮＫで暗号化し、銀行１５に送信する。銀行１５は、自身の秘密鍵ＫＳＢＮＫでこのデータを復号化した後、自身の公開鍵ＫＰＢＮＫにより署名Ｓａを検査することにより、ＩＣカード４５が正当に発行されたものであることを確認する。また、銀行１５は、例えば公開鍵ＫＰＢＮＫと受信したＩＤａとに対し、自身の秘密鍵ＫＳＢＮＫで署名を行い、この署名情報だけをＩＣカード４５に送信する。ＩＣカード４５では、この署名を公開鍵ＫＰＢＮＫで元に戻し、公開情報であるＫＰＢＮＫと自身のＩＤａであることとを検証することにより、署名情報の送信元が正当な銀行１５であることを確認する。

【００８１】このようにして相互認証を行った後、ステップＳ１１５において銀行１５は、乱数ｒａを生成し、一方向性の暗号関数ｆと電子小切手台帳発行時に生成したサービス享受者１１の公開鍵ＫＰＡとにより下記の態様でｒａを暗号化し、ＩＣカード４５に送信する。

【００８２】Ｅｒａ＝ｆ（ｒａ、ＫＰＡ）

その後、ステップＳ１１６において、ＩＣカード４５は、受信したＥｒａを自分の秘密鍵ＫＳＡにより下記のように復号化し、サービス享受者１１に対し電子小切手の振出金額等の入力を要求する。

【００８３】ｒａ＝ｆ＊（ｒａ、ＫＳＡ）

ここでのｆ＊は、関数ｆの逆関数を示す。以下、この明細書において同様の表現は逆関数を示す（但し、各図中では、例えばｆの－１乗のような表現により逆関数を示している）。

【００８４】次に、ステップＳ１１７において、サービス享受者１１は、振出して貰いたい電子小切手の金額と枚数とをＩＣカード４５に通知する。ここでは、５０００円の電子小切手１枚を振出す例で考える。

【００８５】ステップＳ１１８において、ＩＣカード４５は、銀行１５に対し電子小切手の振出しを要求する通信文を生成する。この通信文には少なくとも、ステップＳ１１６において復号化したｒａ、振出要求金額５０００円、振出枚数１枚、電子小切手台帳発行時に格納されたＩＤ番号（ＩＤａ）のデータを含む。

【００８６】更に、ステップＳ１１９において、ＩＣカード４５ではステップＳ１１８で生成した通信文を元に一方向性関数Ｄと秘密鍵ＫＳＡとを使用して、メッセージ認証子ＭＡＣＡを生成する。

【００８７】ＭＡＣＡ＝Ｄ＊（５０００円、１枚、ｒａ、ＩＤＡ、…、ＫＳＡ）

ここで生成したＭＡＣＡを、ステップＳ１１８において生成した通信文に付加する。この実施形態において、上記関数の処理（認証子を求める）は、図８に示すような態様で行う。

【００８８】そして、ステップＳ１２０において、ステップＳ１１９で生成した通信文＋ＭＡＣＡを一方向性の暗号関数Ｆｒｅｑ及び公開鍵ＫＰＢＮＫで下記のように暗号化し、これを銀行１５に送信する。

【００８９】Ｅｒｅｑ＝Ｆｒｅｑ（５０００円の電子小切手１枚の振出要求通信文＋ＭＡＣＡ、ＫＰＢＮＫ）

この実施形態において、上記関数の処理（暗号化／復号化を行う場合）は、図９に示すように暗号化することを示す。また、この実施形態において、＋の演算子は、図９に示すようにデータを連結することを示す。

【００９０】次に、ステップＳ１２１において、暗号文Ｅｒｅｑを受信した銀行１５は、自身の秘密鍵ＫＳＢＮＫにより下記のようにＥｒｅｑを復号化する。

【００９１】５０００円の電子小切手１枚の振出し要求通信文＋ＭＡＣＡ＝Ｆｒｅｑ＊（Ｅｒｅｑ、ＫＳＢＮＫ）

次に、ステップＳ１２２において、復号化した通信文の中からステップＳ１１５で生成したｒａ、振出し要求金額５０００円、振出枚数１枚、電子小切手台帳発行時に格納されたＩＤ番号（ＩＤａ）のデータを取り出し、ＭＡＣＡが正しいことを検証する。

【００９２】この検証は、ＭＡＣＡ´＝Ｄ（５０００円、１枚、ｒａ、ＩＤＡ、…、ＫＰＡ）と、５０００円の電子小切手１枚の振出要求通信文＋ＭＡＣＡ＝Ｆｒｅｑ＊（Ｅｒｅｑ、ＫＳＢＮＫ）とを比較することによって行なわれる。次に、ステップＳ１２３において、認証子ＭＡＣＡが正しいことを確認した銀行１５は、サービス享受者１１の口座１７に振出金額合計以上の残高があることを確認し、提出金額、提出銀行名、提出日時等から成る電子小切手の通信文を要求された振出枚数の通信文を要求された振出枚数分生成させる。この場合、振出枚数は１枚のため通信文は１つとなる。

【００９３】次に、ステップＳ１２４において、１つの通信文についてＮ個の乱数ｒｂｎｋ１～ｒｂｎｋｎを発生させる。但し、乱数ｒｂｎｋ１～ｒｂｎｋｎは、すべて異なる値となるように生成する。ここでは、取り敢えず５個の乱数を発生させることとし、発生した乱数ｒｂｎｋ１～ｒｂｎｋ５の大小関係は、ｒｂｎｋ１＜ｒｂｎｋ２＜ｒｂｎｋ３＜ｒｂｎｋ４＜ｒｂｎｋ５の関係があるものとする。そして、通信文の中から少なくとも振出金額、振出銀行名、提出日時を取り出し、これらのデータに乱数ｒｂｎｋｎを付加し、一方向性関数Ｈと銀行１５の秘密鍵ＫＳＢＮＫとにより下記のようにＮ個のメッセージ認証子ＭＡＣｂｎｋ１～ＭＡＣｂｎｋｎを求める。

【００９４】

ＭＡＣｂｎｋ１＝Ｈ＊（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ５、ＫＳＢＮＫ）

ＭＡＣｂｎｋ２＝Ｈ＊（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ２

、ＫＳＢＮＫ）

ＭＡＣｂｎｋ５＝Ｈ＊（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ５、ＫＳＢＮＫ）

更に、ステップＳ１２５において、ステップＳ１２３で生成した通信文にステップＳ１２４で発生した乱数と認証子を付加し、一方向性関数Ｆｃｈｒとサービス享受者１１の公開鍵ＫＰＡとで下記のように暗号文Ｅｃｈｒを生成する。ここで、乱数ｒｂｎｋｎと認証子ＭＡＣｂｎｋｎは対応が取れるように並べるものとする。

【００９５】Ｅｃｈｒ＝Ｆｃｈｒ（５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋…＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５）

そして、ステップＳ１２６において、このＥｃｈｒをサービス享受者１１のＩＣカード４５へ送信すると共に、サービス享受者１１の口座１７から当該金額（ここでは５０００円）を引き落とし、自行の払出小切手支払いに当てる口座２１に入金しておく。その後、ステップＳ１２７において、ＩＣカード４５は銀行１５から受信したＥｃｈｒを自身の秘密鍵ＫＳＡによって復号化する。

【００９６】５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋…＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５）＝Ｆｃｈｒ＊（Ｅｃｈｒ、ＫＳＡ）

次に、ステップＳ１２８において、「５０００円の電子小切手の振出許可通知文」の中から振出金額、振出銀行名、振出日時等を取り出し、銀行ＢＮＫの公開鍵ＫＰＢＮＫを使用してＭＡＣｂｎｋ１～ＭＡＣｂｎｋ５の署名が確かに銀行ＢＮＫによって行われたものであることを確認する。

【００９７】

ＭＡＣｂｎｋ１´＝Ｈ（５０００円、振出銀行名、提出日時、…、ｒｂｎｋ１、ＫＰＢＮＫ）

ＭＡＣｂｎｋ２´＝Ｈ（５０００円、振出銀行名、提出日時、…、ｒｂｎｋ２、ＫＰＢＮＫ）

ＭＡＣｂｎｋ５´＝Ｈ（５０００円、振出銀行名、提出日時、…、ｒｂｎｋ５、ＫＰＢＮＫ）

上記によって得られたＭＡＣｂｎｋ１´～ＭＡＣｂｎｋ５´とステップＳ１２７でＥｃｈｒを復号化（Ｆｃｈｒ＊（Ｅｃｈｒ、ＫＳＡ））した結果に含まれるＭＡＣｂｎｋ１～ＭＡＣｂｎｋ５が同一であれば、この認証子は銀行１５によって署名されたものと判定する。

【００９８】次に、ステップＳ１２９において、ＩＣカード４５は、ステップＳ１２８によって銀行１５からの「５０００円の電子小切手の振出許可通知文」が確認できれば、５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋……＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５を電子小切手としてＩＣカード４５内に格納しておく。

【００９９】次に、サービス享受者１１からサービス提供者２７に対する電子小切手での支払手順について説明する。

【０１００】図１０、及び図１１は、サービス提供者２７からサービス、商品等の提供を受けたことに対する代金の支払を電子小切手で行う場合の手順を示すフローチャートである。この電子小切手での支払を行う前提として、サービス提供者２７についてもサービス享受者１１におけると同様に、図５～図７で示した手順によって銀行１５が発行したＩＣカード４７を所持しているものとする。従って、ＩＣカード４７にもＩＣカード４５と同様、銀行１５の公開鍵ＫＰＢＮＫ、サービス提供者２７の秘密鍵ＫＳＢ、サービス提供者２７の公開鍵ＫＰＢ、サービス提供者２７の利用者ＩＤ（ＩＤｂ）、利用者ＩＤ（ＩＤｂ）と公開鍵ＫＰＢに対する銀行１５の署名Ｓｂが記憶されている。また、この例では、サービス享受者１１が図７のステップＳ１２９でチャージした電子小切手で支払うものとする。

【０１０１】まず、ステップＳ１３１において、サービス提供者２７はサービス享受者１１にサービス又は商品を提供したことに対する代金支払の請求を行う。次に、ステップＳ１３２において、サービス享受者１１はＩＣカード４５に対し電子小切手の払出指示を行う。その後、ステップＳ１３３において、電子小切手払出指示を受けたＩＣカード４５は、サービス享受者１１に対してサービス享受者１１の本人確認を行う。本人確認の方法は、暗証番号、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せることによって行う。この本人確認の後、ステップＳ１３４において、ＩＣカード４５は自カード内に格納している電子小切手の金額、枚

数、合計金額等をサービス享受者１１に通知すると共にいくら払出すのか、又は、どの電子小切手を払出すのかをサービス享受者１１に問い合せる。

【０１０２】次に、ステップＳ１３５において、サービス享受者１１は、いくら払出すのか、又は、どの電子小切手を払出すのかをＩＣカード４５に指定する。ここでは、ステップＳ１２９でチャージした電子小切手を払出すこととする。次に、ステップＳ１３６において、指定を受けたＩＣカード４５は、金額で指定をされた場合は指定金額以上の残高の電子小切手があることを確認すると共に、ＩＣカード４７に対し電子小切手により支払を行う旨の通知を行う。次に、ステップＳ１３７において、ＩＣカード４５とＩＣカード４７は相互に認証を行うことにより、互いに正当な通信相手であることを確認する。例えば、次のような方法で互いの認証と公開鍵の交換とを行う。ＩＣカード４５は、ＫＳＡ、ＩＤａ、ＳａをＩＣカード４７へ送信する。ＩＣカード４７では、銀行１２５の公開鍵ＫＰＢＮＫにより署名Ｓａを検証することによって、ＩＣカード４５が銀行１５により発行されたものであり、且つ、ＫＳＡ、ＩＤａが正しいことを確認することができる。また、ＩＣカード４７から同様にＫＳＢ、ＩＤｂ、ＳｂをＩＣカード４５に送信することで、ＩＣカード４５は、ＩＣカード４７、及びその公開鍵ＫＰＢの正当性を検証することができる。

【０１０３】次に、ステップＳ１３８において、ＩＣカード４７は、Ｎ個の乱数ｒｂ１～ｒｂｎを生成する。このとき生成する乱数の個数は、図６のステップＳ１２４で生成した乱数の個数と同じ数を生成するものとし、生成した乱数はすべて異なる値になるよう生成する。この例では、５個の乱数ｒｂ１～ｒｂ５を生成し、ｒｂ１、ｒｂ２、ｒｂ３、ｒｂ４、ｒｂ５の順に並べ、一方向性関数ｆｒと公開鍵ＫＰＡとで下記のように暗号化してＩＣカード４５に送信する。

【０１０４】Ｅｒｂ＝ｆｒ（ｒｂ１＋ｒｂ２＋ｒｂ３＋ｒｂ４＋ｒｂ５，ＫＰＡ）

なお、この例では、ｒｂ１～ｒｂ５の大小関係をｒｂ１＜ｒｂ３＜ｒｂ５＜ｒｂ２＜ｒｂ４とする。

【０１０５】次に、ステップＳ１３９において、ＩＣカード４５はＥｒｂを復号化し、ｒｂ１～ｒｂ５と自身のＩＤａ等から一方向性関数Ｇを、また、秘密鍵ＫＳＡから認証子ＭＡＣａを、夫々下記のように生成する。

【０１０６】ｒｂ１＋ｒｂ２＋ｒｂ３＋ｒｂ４＋ｒｂ５＝ｆｒ＊（Ｅｒｂ、ＫＳＡ）

ＭＡＣａ＝Ｇ＊（ｒｂ１、ｒｂ２、ｒｂ３、ｒｂ４、ｒｂ５、ＩＤａ、…、ＫＳＡ）

次に、ステップＳ１４０において、ステップＳ１３９で格納した電子小切手「５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋…＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５」を取出し、受信した乱数ｒｂ１～ｒｂ５の大小関係の順にｒｂｎｋ１＋ＭＡＣｂｎｋ１～ｒｂｎｋ５＋ＭＡＣｂｎｋ５を並べ変える。この例においては、乱数ｒｂｎｋ１～ｒｂｎｋ５の大小関係は、ステップＳ１２４で示した通りｒｂｎｋ１＜ｒｂｎｋ２＜ｒｂｎｋ３＜ｒｂｎｋ４＜ｒｂｎｋ５であるから、

５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３

と並べ変える。

【０１０７】今、ＩＣカード４７から送信されてきた乱数は、ｒｂ１＜ｒｂ３＜ｒｂ５＜ｒｂ２＜ｒｂ４であるから、仮に、ｒｂ１＝１、ｒｂ２＝４、ｒｂ３＝２、ｒｂ４＝５、ｒｂ５＝３とすると、銀行１５から受領したｒｂｎｋ１～ｒｂｎｋ５は、ｒｂｎｋ１＜ｒｂｎｋ２＜ｒｂｎｋ３＜ｒｂｎｋ４＜ｒｂｎｋ５となる。よって、これをｒｂｎｋ１、ｒｂｎｋ４、ｒｂｎｋ２、ｒｂｎｋ５、ｒｂｎｋ３の順に並べ変えることとなる。

【０１０８】次に、ステップＳ１４１において、ステップＳ１４０で並べ変えた電子小切手に、ステップＳ１３９で生成したＭＡＣａとＩＤａとを加え、一方向性関数ＦｐａｙとサービスＳ提供者２７の公開鍵ＫＰＢとで下記のように暗号文Ｅｐａｙを生成する。

【０１０９】Ｅｐａｙ＝Ｆｐａｙ（５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３＋ＭＣＡＣａ＋ＩＤａ、ＫＰＢ）

次に、ステップＳ１４２において、ＩＣカード４５は、ＩＣカード４７に暗号文Ｅｐａｙを送信する。ＩＣカード４５は、暗号文Ｅｐａｙが正常にＩＣカード４７に届いたことが確認されれば、送信した電子小切手「５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋…＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５」を無効化する。

【０１１０】次に、ステップＳ１４３において、暗号文Ｅｐａｙを受信したＩＣカード４７は、秘密鍵ＫＳＢにより暗号文Ｅｐａｙを復号化する。

【０１１１】５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３＋ＭＣＡＣａ＋ＩＤａ＝Ｆｐａｙ＊（Ｅｐａｙ、ＫＳＢ）

暗号文Ｅｐａｙを復号化した後、ステップＳ１４４において、ＩＣカード４７はステップＳ１３８で生成した乱数ｒｂ１～ｒｂ５、ＩＤａ等からＩＣカード４５の公開鍵ＫＰＡと署名を行うための一方向性関数Ｇとから下記のようにしてＩＣカード４５の署名を確認する。

【０１１２】ＭＡＣａ´＝Ｇ（ｒｂ１、ｒｂ２、ｒｂ３、ｒｂ４、ｒｂ５、ＩＤａ、…、ＫＰＡ）

そして、ＭＡＣａ゛とステップＳ１４３で得られたＭＡＣａとを比較し、同一であればＩＣカード４５による署名がされたものであると認識する。

【０１１３】次に、ステップＳ１４５において、ステップＳ１３８でＩＣカード４５に送信した乱数ｒｂ１～ｒｂ５の大小関係から、ステップＳ１４３で暗号文Ｅｐａｙを復号化した際に得られたｒｂｎｋ１～ｒｂｎｋ５の大小関係の並びが正しいことを確認する。この例では、送信したｒｂ１～ｒｂ５の大小関係がｒｂ１＜ｒｂ３＜ｒｂ５＜ｒｂ２＜ｒｂ４であったため、ｒｂｎｋ１～ｒｂｎｋ５がｒｂｎｋ１、ｒｂｎｋ４、ｒｂｎｋ２、ｒｂｎｋ５、ｒｂｎｋ３の順序で並んでいることを確認する。もし、ここで乱数ｒｂｎｋ１～ｒｂｎｋ５の並び順がステップＳ１３８でＩＣカード４５に送信した順序と異なっていた場合は、銀行１５が正当に発行したＩＣカード４５の中から送信されたものではなく不正使用された電子小切手であるとしてサービス提供者２７に通知すると共に以降の支払手順を停止する。

【０１１４】更に、次のステップＳ１４６において、ＩＣカード４７は「５０００円の電子小切手の振出許可通知文」の中から振出金額、振出銀行名、振出日時等を取出し、振出銀行名から自身が記憶している銀行１５の公開鍵ＫＰＢＮＫを得る。そして、この公開鍵ＫＰＢＮＫを使用してＭＡＣｂｎｋ１～５の署名が確かに銀行１５によって行われたものであることを確認する。

【０１１５】

ＭＡＣｂｎｋ１゛＝Ｈ（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ１、ＫＰＢＮＫ）

ＭＡＣｂｎｋ４゛＝Ｈ（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ４、ＫＰＢＮＫ）

．
．
．

ＭＡＣｂｎｋ３゛＝Ｈ（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ３、ＫＰＢＮＫ）

上記によって得られたＭＡＣｂｎｋ１゛～ＭＡＣｂｎｋ５゛と、ステップＳ１４３でＥｐａｙを復号化（Ｆｐａｙ＊（Ｅｐａｙ、ＫＳＢ））した結果に含まれるＭＡＣｂｎｋ１～ＭＡＣｂｎｋ５とが同一であれば、この認証子は銀行１５によって署名されたものと判断する。

【０１１６】次に、ステップＳ１４７において、銀行１５の署名が確認されれば、ＩＣカード４７は受領した電子小切手の金額をサービス提供者２７に通知する。そして、５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３を電子小切手として格納する。

【０１１７】次に、サービス提供者２７が銀行１５に対し、上記電子小切手を用いて決済を行う手順について説明する。

【０１１８】図１２、及び図１３は、サービス提供者２７がサービス享受者１１から受領した５０００円の電子小切手を銀行１５に呈示し、決済を行う際の手順を示すフローチャートである。

【０１１９】まず、ステップＳ１５１において、サービス提供者２７は、電子小切手台帳であるＩＣカード４７が使用できる銀行１５のＡＴＭ又は銀行１５と通信が可能で、且つ、電子小切手台帳であるＩＣカード４７が使用可能な端末機を経由してＩＣカード４７に対し電子小切手の決済要求を行う。

【０１２０】次に、ステップＳ１５２において、電子小切手払出指示を受けたＩＣカード４７は、サービス提供者２７に対してサービス提供者２７の本人確認を行う。本人確認の方法は、暗証番号、声紋、指紋等による生物学的特徴を利用した方法等を単独又は組合せることによって行う。

【０１２１】この本人確認の後、ステップＳ１５３において、ＩＣカード４７は自カード内に格納している電子小切手の振出銀行、提出日、金額、枚数、合計金額等をサービス提供者２７に通知すると共に、どの電子小切手を決済するのかをサービス提供者２７に問い合せる。次に、ステップＳ１５４において、サービス提供者２７は決済する電子小切手をＩＣカード４７に指定する。ここでは、サービス享受者１１から支払を受けた銀行１５振出の５０００円の電子小切手（図１０及び図１１参照）の決済を行うものとする。次に、ステップＳ１５５において、指定を受けたＩＣカード４７は、銀行１５に対し電子小切手の決済を行う旨の通知を行う。

【０１２２】その後、ステップＳ１５６において、ＩＣカード４と銀行１５とは、相互に認証を行うことにより互いに正当な通信相手であることを確認する。ここでは、図６のステップＳ１１４と同様にＩＣカード４７からは、ＫＳＢ、ＩＤｂ、Ｓｂを銀行１５に送信する。また、銀行１５は、公開鍵ＫＰＢＮＫと受信したＩＤｂに対し、自身の秘密鍵ＫＳＢＮＫで署名を行い、この署名情報だけをＩＣカード４７に送信することで相互の認証を行うことができる。

【０１２３】次に、ステップＳ１５７において、銀行１５は、Ｎ個の乱数ｒｇ１～ｒｇｎを生成する。このとき生成する乱数の個数は、ステップＳ１２４で生成した乱

数の個数と同じ数を生成するものとし、生成した乱数はすべて異なる値になるように生成する。この例では、５個の乱数ｒｇ１～ｒｇ５を生成し、ｒｇ１、ｒｇ２、ｒｇ３、ｒｇ４、ｒｇ５の順に並べ、一方向性関数ｆｒｇと公開鍵ＫＰＢとで下記のように暗号化して、順にＩＣカード４７に送信する。

【０１２４】Ｅｒｇ＝ｆｒ（ｒｂ１＋ｒｂ２＋ｒｂ３＋ｒｂ４＋ｒｂ５、ＫＰＡ）

なお、この例では、ｒｇ１～ｒｇ５の大小関係をｒｇ４＜ｒｇ１＜ｒｇ２＜ｒｇ５＜ｒｇ３とする。

【０１２５】次に、ステップＳ１５８において、ＩＣカード４７はＥｒｇを復号化し、受信したｒｇ１～ｒｇ５と自身のＩＤｂ等から一方向性関数Ｇを、秘密鍵ＫＳＢから認証子ＭＡＣｂを、夫々下記のように生成する。

【０１２６】ｒｂ１＋ｒｂ２＋ｒｂ３＋ｒｂ４＋ｒｂ５＝ｆｒ＊（Ｅｒｂ、ＫＳＡ）

ＭＡＣｂ＝Ｇ＊（ｒｇ１、ｒｇ２、ｒｇ３、ｒｇ４、ｒｇ５、ＩＤｂ、…、ＫＳＢ）

次に、ステップＳ１５９において、ステップＳ１５７で格納した電子小切手「５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋…＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５」を取出し、受信した乱数ｒｇ１～ｒｇ５の大小関係の順にｒｂｎｋ１＋ＭＡＣｂｎｋ１～ｒｂｎｋ５＋ＭＡＣｂｎｋ５を並べ変える。この例においては、ｒｂｎｋ１～ｒｂｎｋ５の大小関係は、ステップＳ１２４で示した通り、ｒｂｎｋ１＜ｒｂｎｋ２＜ｒｂｎｋ３＜ｒｂｎｋ４＜ｒｂｎｋ５であるから、

５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４

と並べ変える。

【０１２７】今、ＩＣカード４７から送信されてきた乱数は、ｒｇ４＜ｒｇ１＜ｒｇ２＜ｒｇ５＜ｒｇ３であるから、仮に、ｒｂ１＝２、ｒｂ２＝３、ｒｂ３＝５、ｒｂ４＝１、ｒｂ５＝４とすると、サービス享受者１１から受領した銀行１５の乱数ｒｂｎｋ１～ｒｂｎｋ５は、ｒｂｎｋ１＜ｒｂｎｋ２＜ｒｂｎｋ３＜ｒｂｎｋ４＜ｒｂｎｋ５である。よって、ｒｂｎｋ２、ｒｂｎｋ３、ｒｂｎｋ５、ｒｂｎｋ１、ｒｂｎｋ４の順に並べ変える。

【０１２８】次に、ステップＳ１６０において、ステップＳ１５９で並べ変えた電子小切手に、ステップＳ１５７で生成したＭＡＣｂとＩＤｂとを加え、一方向性関数ＦａｃｃとＩＣカード４７に記憶されている銀行１５の公開鍵ＫＰＢＮＫとで暗号文Ｅａｃｃを生成する。

【０１２９】Ｅａｃｃ＝Ｆａｃｃ（５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４＋ＭＣＡＣｂ＋ＩＤｂ、ＫＰＢＮＫ）

次に、ステップＳ１６１において、ＩＣカード４７は、銀行１５に暗号文Ｅａｃｃを送信する。ＩＣカード４７は、この暗号文Ｅａｃｃが正常に銀行１５に届いたことを確認すると、送信した電子小切手「５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋…ｒｂｎｋ５＋ＭＡＣｂｎｋ５」を無効化する。次に、ステップＳ１６２において、暗号文Ｅａｃｃを受信した銀行１５は、秘密鍵ＫＳＢＮＫにより、この暗号文Ｅａｃｃを下記のように復号化する。

【０１３０】５０００円の電子小切手の振出許可通知文＋ｒｂｎｋ２＋ＭＡＣｂｎｋ２＋ｒｂｎｋ３＋ＭＡＣｂｎｋ３＋ｒｂｎｋ５＋ＭＡＣｂｎｋ５＋ｒｂｎｋ１＋ＭＡＣｂｎｋ１＋ｒｂｎｋ４＋ＭＡＣｂｎｋ４＋ＭＣＡＣｂ＋ＩＤｂ＝Ｆａｃｃ＊（Ｅａｃｃ、ＫＳＢＮＫ）

このようにして暗号文Ｅａｃｃを復号化した銀行１５は、ステップＳ１６３において、復号化したデータのＩＤｂからＩＣカード４７の公開鍵ＫＰＢを検索し、ステップＳ１５７で生成した乱数ｒｇ１～ｒｇ５、ＩＤｂ等から下記のようにＩＣカード４７の署名を確認する。

【０１３１】ＭＡＣｂ´＝Ｇ（ｒｇ１、ｒｇ２、ｒｇ３、ｒｇ４、ｒｇ５、ＩＤｂ、…、ＫＰＢ）

このＭＡＣｂ´と、ステップＳ１６２で得られたＭＡＣｂとを比較し、同一であればＩＣカード４７の署名がされたものであると判断する。

【０１３２】次に、ステップＳ１６４において、ステップＳ１５７でＩＣカード４７に送信した乱数ｒｇ１～ｒｇ５の大小関係からステップＳ１６２で暗号文Ｅａｃｃを復号化した際に得られたｒｂｎｋ１～ｒｂｎｋ５の大小関係の並びが正しいことを確認する。この例では、送信したｒｇ１～ｒｇ５の大小関係がｒｇ４＜ｒｇ１＜ｒｇ２＜ｒｇ５＜ｒｇ３であったため、ｒｂｎｋ１～ｒｂｎｋ５がｒｂｎｋ２、ｒｂｎｋ３、ｒｂｎｋ５、ｒｂｎｋ１、ｒｂｎｋ４の順序で並んでいることを確認する。もし、ここで乱数ｒｂｎｋ１～ｒｂｎｋ５の並び順がステップＳ１５７でＩＣカード４７に送信した順序と異なる順番で受信した場合、銀行１５が正当に発行したＩＣカード４７の中から送信されたものではなく、不正使用された電子小切手として銀行１５は、以降の決済手順を停止する。

【０１３３】更に、ステップＳ１６５において、銀行１５は、自身の公開鍵ＫＰＢＮＫを使用して下記のようにＭＡＣｂｎｋ１～５の署名を確認し、確かに自分自身によって振り出されたものであることを確認する。

【０１３４】

ＭＡＣｂｎｋ２´＝Ｈ（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ２、ＫＰＢＮＫ）

ＭＡＣｂｎｋ３＝Ｈ（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ３、ＫＰＢＮＫ）

ＭＡＣｂｎｋ４＝Ｈ（５０００円、振出銀行名、振出日時、…、ｒｂｎｋ４、ＫＰＢＮＫ）

次に、ステップＳ１６６において、銀行１５は、自身が振り出した小切手であることが確認できれば、ステップＳ１２６で入金した自行の払出小切手支払に当てる口座２１からサービス提供者２７の口座３５に５０００円を振替え、その旨をＩＣカード４７に通知する。そして、次のステップＳ１６７において、ＩＣカード４７は、銀行１５からの通知内容をサービス提供者２７に通知する。

【０１３５】上述した実施形態では、説明を単純化するために図２の簡単化した電子小切手システムを例に取ったが、サービス提供者２７はサービス享受者１１から受領した電子小切手を図１０及び図１１に示した手順を実行することで、銀行１５が発行したＩＣカード（図示しない）を有する別の第三者（図示しない）に対しても支払うことができる。また、サービス提供者２７が複数種類の金種の電子小切手を有する場合に、サービス享受者１１から支払われた電子小切手に対して、ステップＳ１４７～Ｓ１５７で示した手順を逆方向に実行することでサービス提供者１１はサービス享受者２７に対しておつりを支払うこともできる。なお、この実施形態では、Ｆｃｈｒ、Ｆｐａｙ、ｆａｃｃについては、ＲＳＡ暗号方式のような安全性が確認されている公開鍵暗号方式を使用する方式としたが、暗号化に使用する鍵を一定期間毎（又はトランザクション毎）に変更するのであれば、ＤＥＳやＦＥＡＬ等の共通鍵暗号方式を用いることもできる。

【０１３６】また、署名を行う際に使用する関数（署名を確認する際に使用する関数）Ｄ＊、Ｈ＊、Ｇ＊は、特開昭６０－２６３７８号公報（ディジタル署名方式）等に開示されている方法で署名を行うことができる。

【０１３７】また、この実施形態においては、正規に銀行１５が発行したＩＣカード４５、４７であることの確認として、これらＩＣカードのＩＤと公開鍵とに対して、銀行１５の署名により、その正当性を確認したが、システムに共通の秘密情報を夫々のＩＣカードが有することをゼロ知識証明法等で確認することでも可能である。

【０１３８】以上、この実施形態で示したように、銀行１５が振出した電子小切手のデータは、他人に支払う時点でのデータの順序の並び変えが発生するが、データそのものを加工する訳ではないので、受領した側も振出人の署名を確実に確認できる。また、受取側も第三者に対して受領した電子小切手で支払を行うことができる。

【０１３９】また、銀行を振出人とする電子小切手とすることで、その署名を確認するための公開鍵は、電子小切手の受取人共通となるため、鍵の管理が非常に容易となる。更には、銀行の公開鍵は、ＩＣカード発行時に記憶させておけば、銀行の署名確認時、銀行や第三者の信用機関へ問い合せる必要がない。

【０１４０】なお、上述した内容は、あくまで本発明の一実施形態に関するものであって、本発明が上記内容のみに限定されることを意味するものでないのは勿論である。

【図面の簡単な説明】

【図１】従来の電子小切手システムを示すブロック図。

【図２】本発明の一実施形態に係る電子小切手システムを示すブロック図。

【図３】一実施形態に係る電子小切手システムの構成要素を示す拡大図。

【図４】銀行からサービス享受者のＩＣカード１５に送信される暗号化データを示した説明図。

【図５】システム利用に際して必要な電子小切手帳の発行手順を示すフローチャート。

【図６】サービス享受者の銀行に対する電子小切手の振出依頼の手順を示すフローチャート。

【図７】サービス享受者の銀行に対する電子小切手の振出依頼の手順を示すフローチャート。

【図８】銀行に送信する通信文に付加する認証子を求めるための処理手順を示すブロック図。

【図９】銀行に送信する通信文を暗号化する場合の処理手順を示すブロック図。

【図１０】サービス提供者に対する電子小切手での支払手順を示すフローチャート。

【図１１】サービス提供者に対する電子小切手での支払手順を示すフローチャート。

【図１２】サービス提供者と銀行間での電子小切手による決済手順を示すフローチャート。

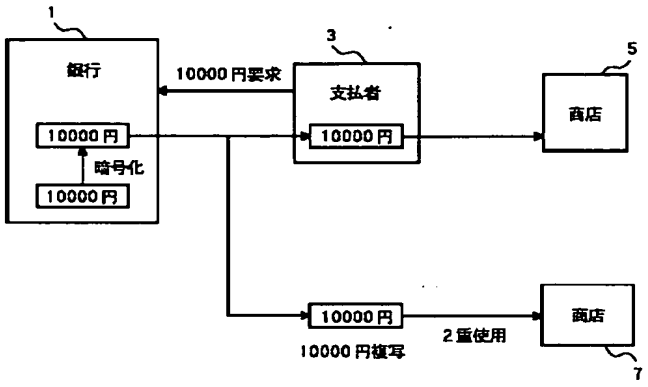
【図１３】サービス提供者と銀行間での電子小切手による決済手順を示すフローチャート。

【符号の説明】

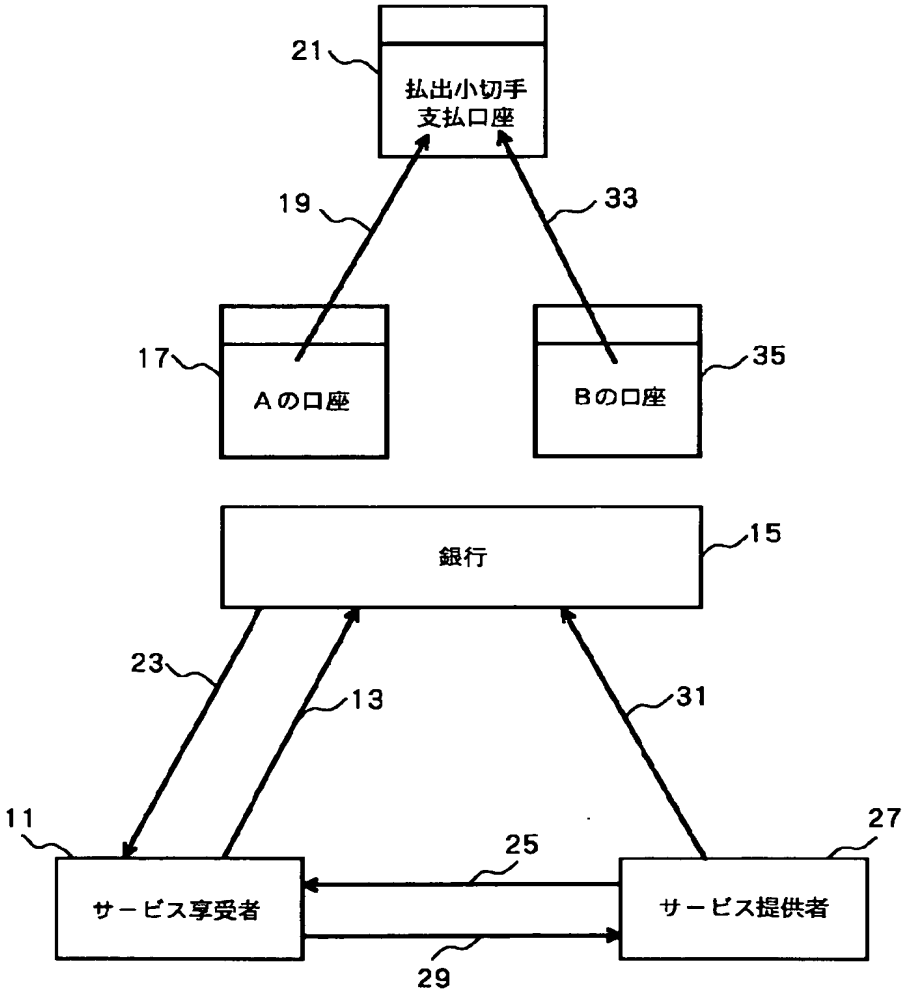
１１　サービス享受者
１５　銀行
１７　サービス享受者の銀行口座
２１　銀行１５の払出小切手支払口座

２７　サービス提供者
３５　サービス提供者の銀行口座
４１、４３　端末機
４５、４７　ＩＣカード

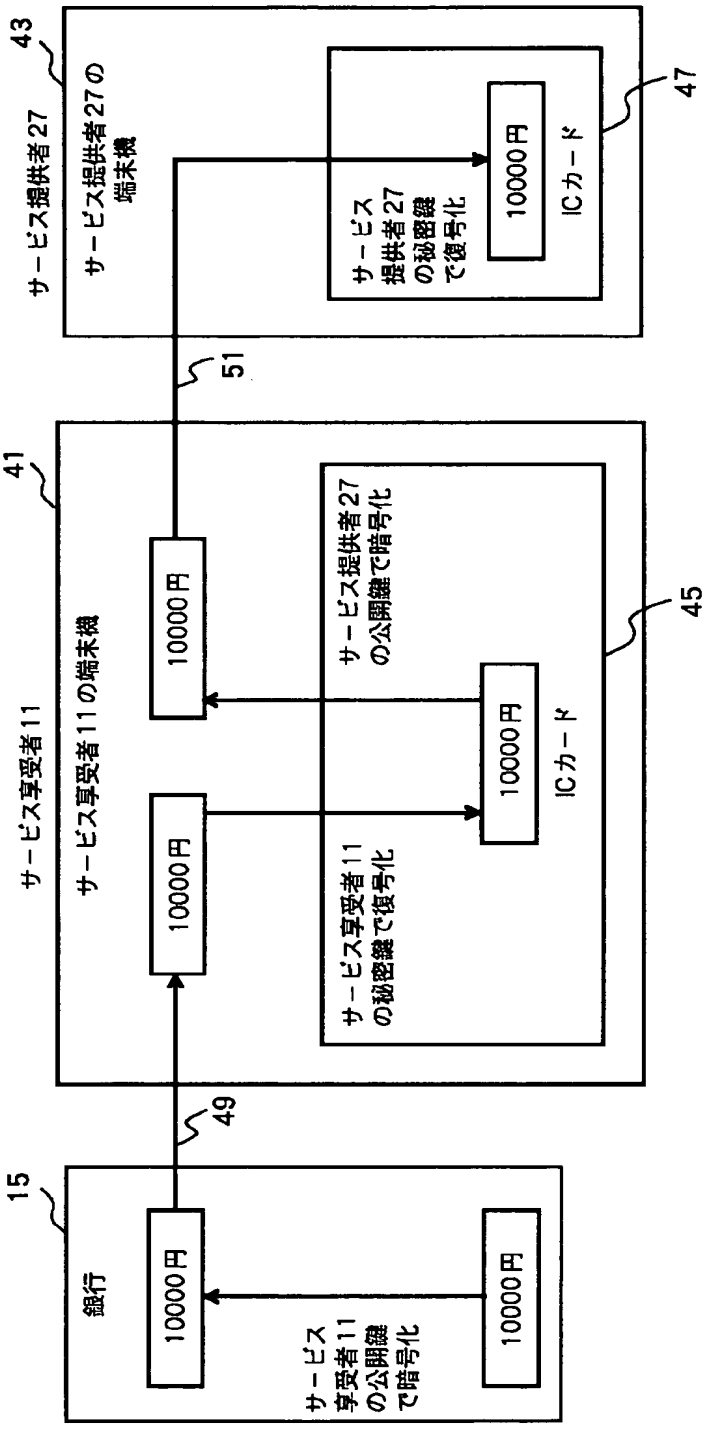
【図１】



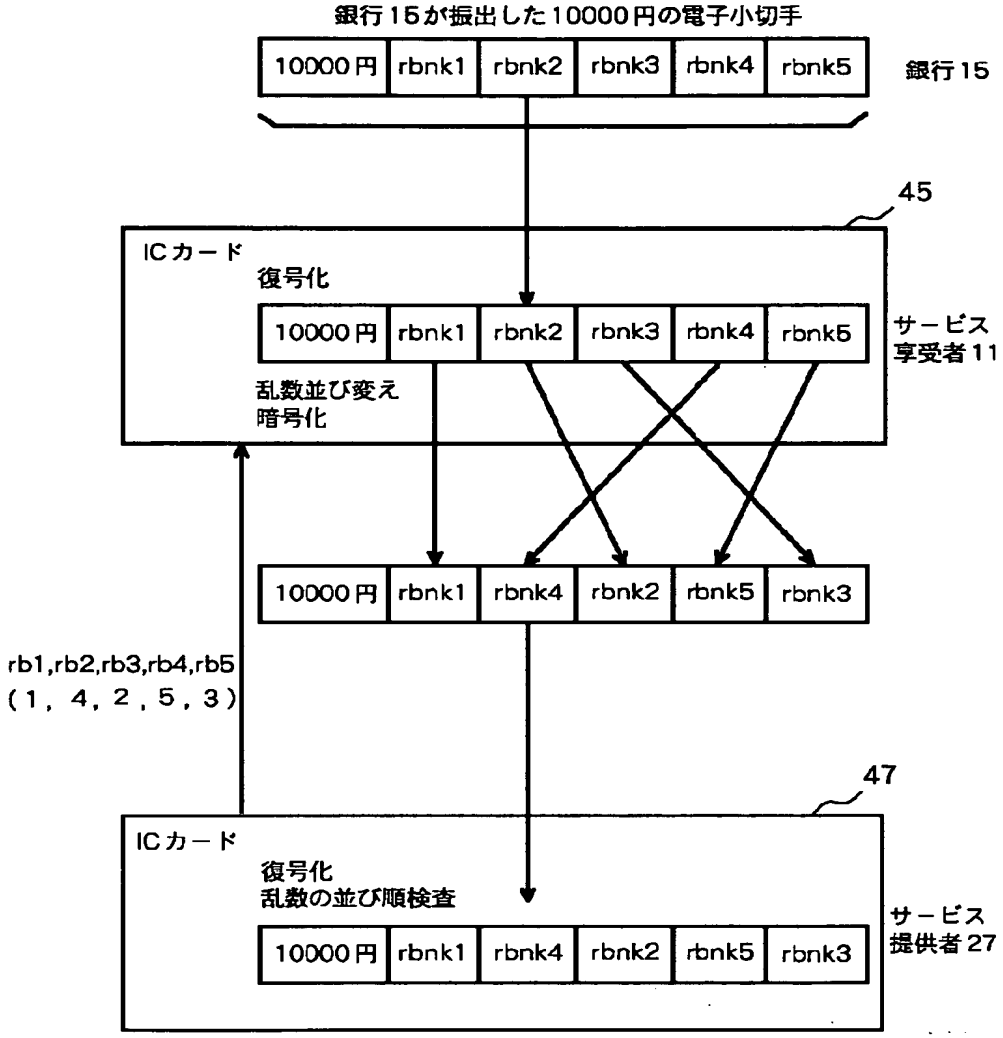
【図２】



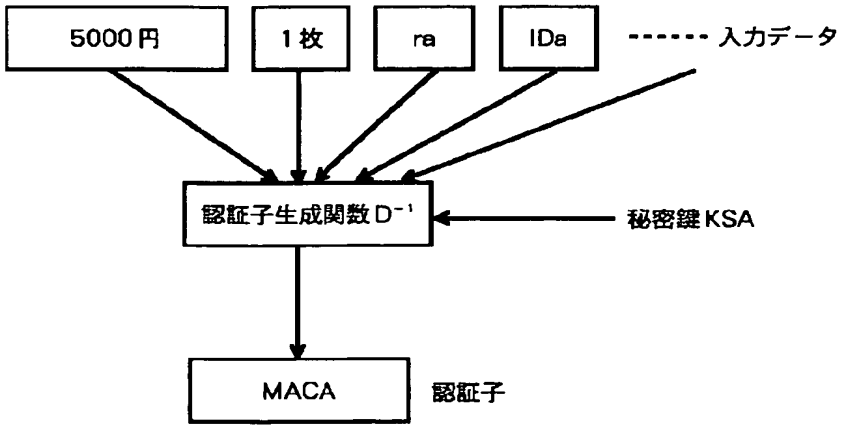
【図3】


43
サービス提供者27
サービス提供者27の端末機
47
サービス提供者27の秘密鍵で復号化
10000円
ICカード
51
41
サービス享受者11
サービス享受者11の端末機
10000円
サービス提供者27の公開鍵で暗号化
45
10000円
ICカード
10000円
サービス享受者11の秘密鍵で復号化
49
15
銀行
10000円
10000円
サービス享受者11の公開鍵で暗号化

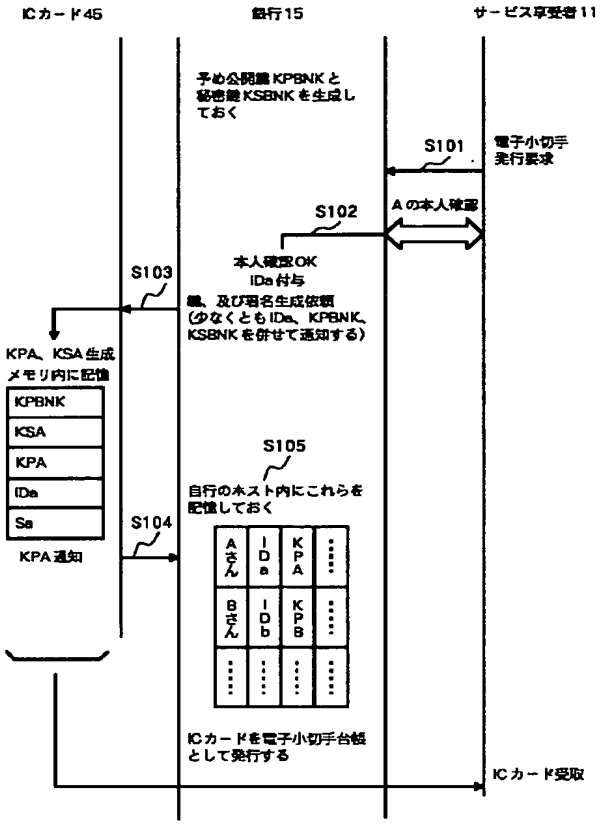
【図4】


銀行15が振出した10000円の電子小切手
10000円
rbnk1
rbnk2
rbnk3
rbnk4
rbnk5
銀行15
45
ICカード
復号化
サービス
享受者11
乱数並び変え
暗号化
rb1,rb2,rb3,rb4,rb5
（1，4，2，5，3）
47
ICカード
復号化
乱数の並び順検査
サービス
提供者27

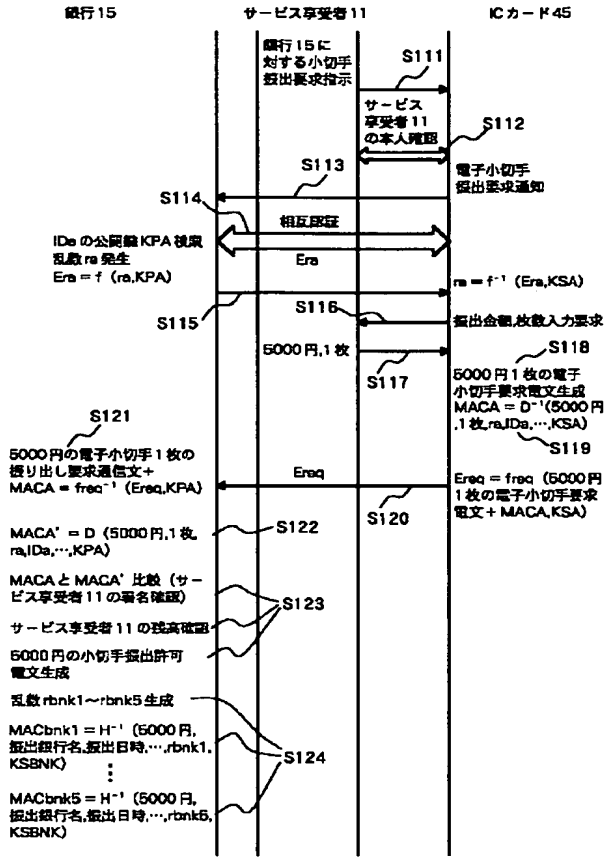
【図8】


5000円
1枚
ra
IDa
------ 入力データ
認証子生成関数 D^{-1}
秘密鍵KSA
MACA
認証子

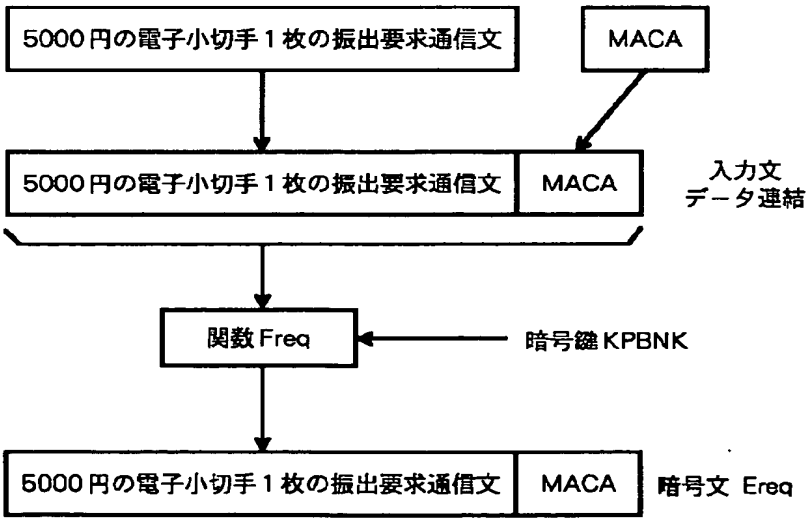
【図5】


ICカード45
銀行15
サービス享受者11
予め公開鍵KPBNKと秘密鍵KSBNKを生成しておく
S101
電子小切手発行要求
S102
Aの本人確認
本人確認OK
IDa付与
S103
鍵、及び署名生成依頼
(少なくともIDa、KPBNK、KSBNKを併せて通知する)
KPA、KSA生成
メモリ内に記憶
KPBNK
KSA
KPA
IDa
Sa
S104
KPA通知
S105
自行のホスト内にこれらを記憶しておく
Aさん
IDa
KPA
Bさん
IDb
KPB
ICカードを電子小切手台帳として発行する
ICカード受取

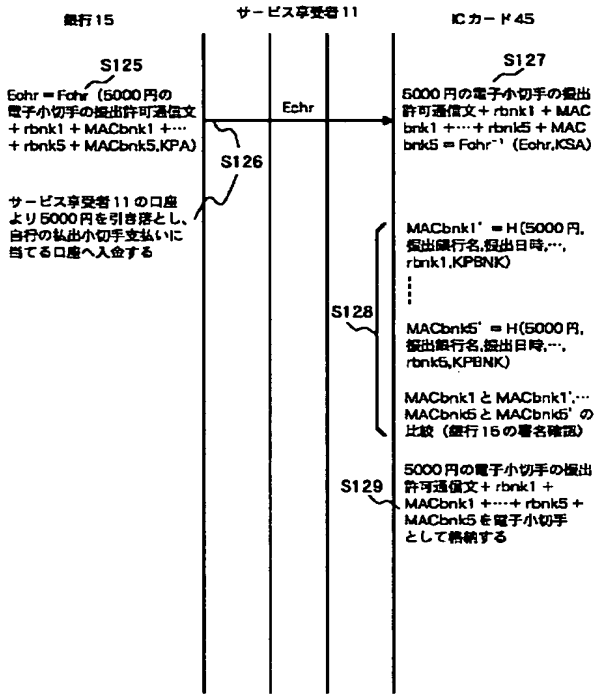
【図6】


銀行15
サービス享受者11
ICカード45
銀行15に対する小切手振出要求指示
S111
サービス享受者11の本人確認
S112
電子小切手振出要求通知
S113
S114
相互認証
IDaの公開鍵KPA検索
乱数ra発生
Era＝f（ra,KPA）
Era
ra＝f⁻¹（Era,KSA）
S115
S116
振出金額,枚数入力要求
5000円,1枚
S117
S118
5000円1枚の電子小切手要求電文生成
MACA＝D⁻¹(5000円,1枚,ra,IDa,…,KSA)
S119
S120
Ereq＝freq（5000円1枚の電子小切手要求電文＋MACA,KSA）
Ereq
S121
5000円の電子小切手1枚の振り出し要求通信文＋MACA＝freq⁻¹（Ereq,KPA）
S122
MACA'＝D（5000円,1枚,ra,IDa,…,KPA）
MACAとMACA'比較（サービス享受者11の署名確認）
S123
サービス享受者11の残高確認
5000円の小切手振出許可電文生成
乱数rbnk1～rbnk5生成
MACbnk1＝H⁻¹（5000円,振出銀行名,振出日時,…,rbnk1,KSBNK）
S124
MACbnk5＝H⁻¹（5000円,振出銀行名,振出日時,…,rbnk5,KSBNK）

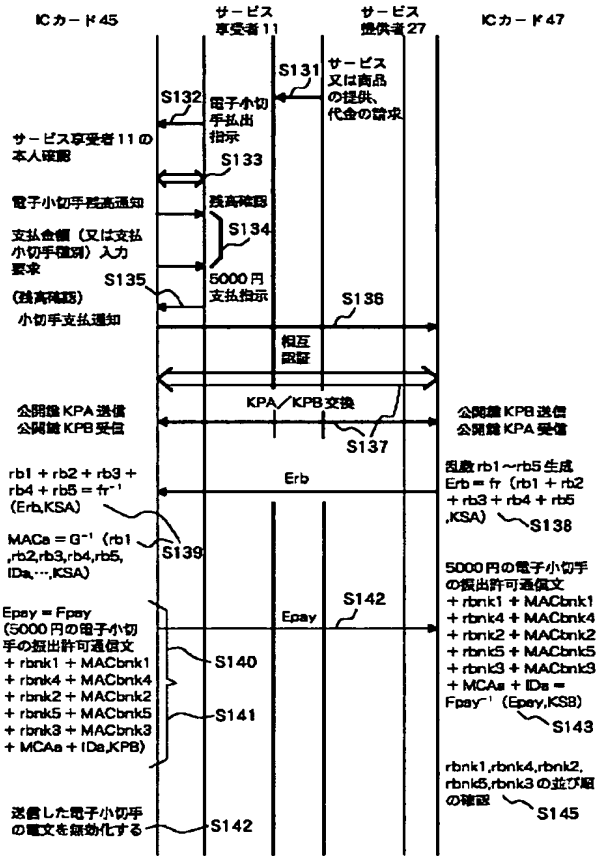
【図9】


5000円の電子小切手1枚の振出要求通信文
MACA
5000円の電子小切手1枚の振出要求通信文
MACA
入力文
データ連結
関数Freq
暗号鍵KPBNK
5000円の電子小切手1枚の振出要求通信文
MACA
暗号文 Ereq

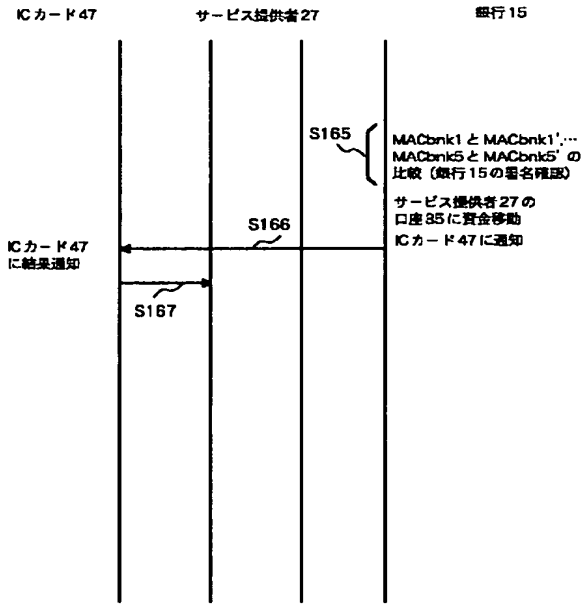
【図7】


銀行15
サービス享受者11
ICカード45
S125
Eohr＝Fohr（5000円の電子小切手の振出許可通信文＋rbnk1＋MACbnk1＋…＋rbnk5＋MACbnk5,KPA）
Echr
S127
5000円の電子小切手の振出許可通信文＋rbnk1＋MACbnk1＋…＋rbnk5＋MACbnk5＝Fohr⁻¹（Eohr,KSA）
S126
サービス享受者11の口座より5000円を引き落とし、自行の払出小切手支払いに当てる口座へ入金する
S128
MACbnk1'＝H(5000円,振出銀行名,振出日時,…,rbnk1,KPBNK)
MACbnk5'＝H(5000円,振出銀行名,振出日時,…,rbnk5,KPBNK)
MACbnk1とMACbnk1',…MACbnk5とMACbnk5'の比較（銀行15の署名確認）
S129
5000円の電子小切手の振出許可通信文＋rbnk1＋MACbnk1＋…＋rbnk5＋MACbnk5を電子小切手として格納する

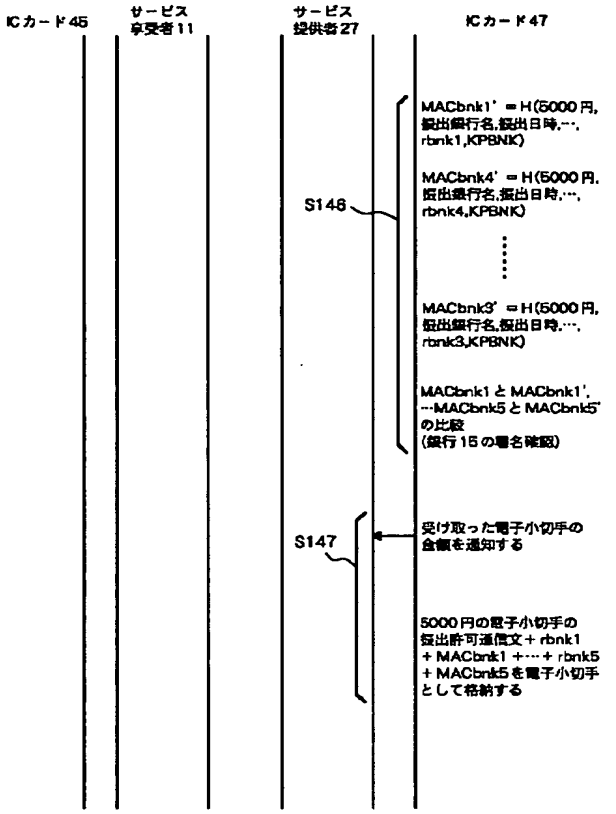
【図10】


ICカード45
サービス享受者11
サービス提供者27
ICカード47
S131
サービス又は商品の提供、代金の請求
S132
電子小切手払出指示
サービス享受者11の本人確認
S133
電子小切手残高通知
残高確認
S134
支払金額（又は支払小切手種別）入力要求
S135
5000円支払指示
（残高確認）
小切手支払通知
S136
相互認証
KPA／KPB交換
公開鍵KPA送信
公開鍵KPB受信
S137
公開鍵KPB送信
公開鍵KPA受信
乱数rb1～rb5生成
Erb＝fr（rb1＋rb2＋rb3＋rb4＋rb5,KSA）
S138
rb1＋rb2＋rb3＋rb4＋rb5＝fr⁻¹（Erb,KSA）
Erb
MACa＝G⁻¹（rb1,rb2,rb3,rb4,rb5,IDa,…,KSA）
S139
Epay＝Fpay（5000円の電子小切手の振出許可通信文＋rbnk1＋MACbnk1＋rbnk4＋MACbnk4＋rbnk2＋MACbnk2＋rbnk5＋MACbnk5＋rbnk3＋MACbnk3＋MCAa＋IDa,KPB）
S140
S141
Epay
S142
5000円の電子小切手の振出許可通信文＋rbnk1＋MACbnk1＋rbnk4＋MACbnk4＋rbnk2＋MACbnk2＋rbnk5＋MACbnk5＋rbnk3＋MACbnk3＋MCAa＋IDa＝Fpay⁻¹（Epay,KSB）
S143
rbnk1,rbnk4,rbnk2,rbnk5,rbnk3の並び順の確認
S145
送信した電子小切手の電文を無効化する
S142

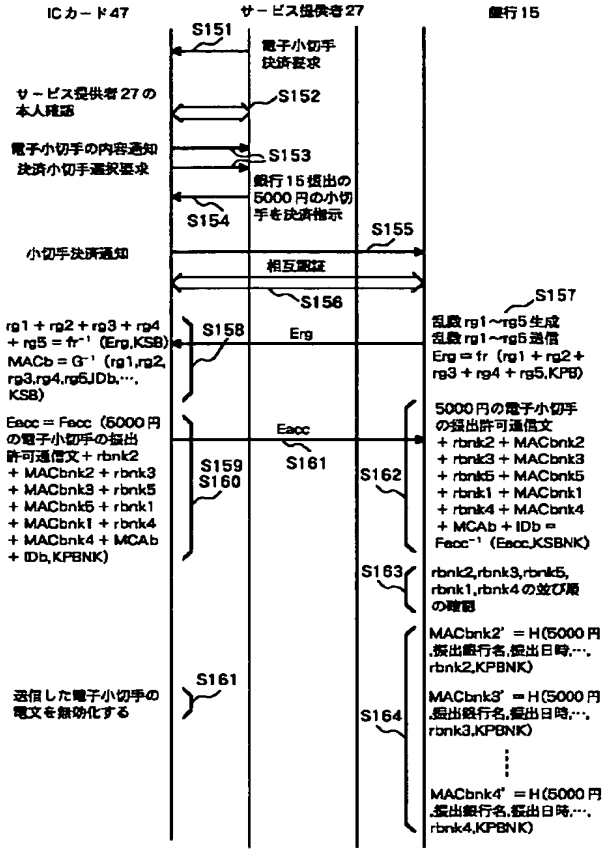
【図13】


ICカード47
サービス提供者27
銀行15
S165
MACbnk1とMACbnk1',…MACbnk5とMACbnk5'の比較（銀行15の署名確認）
サービス提供者27の口座85に資金移動
S166
ICカード47に通知
ICカード47に結果通知
S167

【図11】


ICカード45
サービス享受者11
サービス提供者27
ICカード47
MACbnk1' ＝H(5000円,振出銀行名,振出日時,…,rbnk1,KPBNK)
MACbnk4' ＝H(5000円,振出銀行名,振出日時,…,rbnk4,KPBNK)
S148
MACbnk3' ＝H(5000円,振出銀行名,振出日時,…,rbnk3,KPBNK)
MACbnk1とMACbnk1',…MACbnk5とMACbnk5'の比較(銀行15の署名確認)
S147
受け取った電子小切手の金額を通知する
5000円の電子小切手の振出許可通信文＋rbnk1＋MACbnk1＋…＋rbnk5＋MACbnk5を電子小切手として格納する

【図12】


ICカード47
サービス提供者27
銀行15
S151
電子小切手決済要求
サービス提供者27の本人確認
S152
電子小切手の内容通知
決済小切手選択要求
S153
銀行15振出の5000円の小切手を決済指示
S154
S155
小切手決済通知
相互認証
S156
S157
乱数rg1～rg5生成
乱数rg1～rg5送信
Erg＝fr（rg1＋rg2＋rg3＋rg4＋rg5,KPB）
rg1＋rg2＋rg3＋rg4＋rg5＝fr⁻¹（Erg,KSB）
S158
Erg
MACb＝G⁻¹（rg1,rg2,rg3,rg4,rg5,IDb,…,KSB）
Eacc＝Fecc（5000円の電子小切手の振出許可通信文＋rbnk2＋MACbnk2＋rbnk3＋MACbnk3＋rbnk5＋MACbnk5＋rbnk1＋MACbnk1＋rbnk4＋MACbnk4＋MCAb＋IDb,KPBNK）
Eacc
S159
S160
S161
5000円の電子小切手の振出許可通信文＋rbnk2＋MACbnk2＋rbnk3＋MACbnk3＋rbnk5＋MACbnk5＋rbnk1＋MACbnk1＋rbnk4＋MACbnk4＋MCAb＋IDb＝Fecc⁻¹（Eacc,KSBNK）
S162
S163
rbnk2,rbnk3,rbnk5,rbnk1,rbnk4の並び順の確認
S161
送信した電子小切手の電文を無効化する
MACbnk2' ＝H(5000円,振出銀行名,振出日時,…,rbnk2,KPBNK)
MACbnk3' ＝H(5000円,振出銀行名,振出日時,…,rbnk3,KPBNK)
S164
MACbnk4' ＝H(5000円,振出銀行名,振出日時,…,rbnk4,KPBNK)